VENTH
ITION

une Disque
n
d Son

Aprete Ma

pli

tioe
e
ns m
atique

s

Discret Mathématiques

et son Applications

Septième édition

Kenneth H. Rosen
Université de Monmouth
(et anciennement AT&T Laboratories)

MATHÉMATIQUES DISCRETES ET SES APPLICATIONS, SEPTIÈME ÉDITION

Publié par McGraw-Hill, une unité commerciale de The McGraw-Hill Companies, Inc., 1221 Avenue of the Amériques, New York, NY 10020.

Ce livre est imprimé sur du papier sans acide.

1 2 3 4 5 6 7 8 9 0 DOW / DOW 1 0 9 8 7 6 5 4 3 2 1

ISBN 978-0-07-338309-5
MHID 0-07-338309-0

Vice-président et rédacteur en chef: *Marty Lange*
Directeur éditorial: *Michael Lange*
Éditeur mondial: *Raghothaman Srinivasan*
Rédacteur en chef: *Bill Stenquist*
Rédacteurs en chef du développement: *Lorraine K. Buczek / Rose Kernan*
Responsable marketing senior: *Curt Reynolds*
Gestionnaire de projet: *Robin A. Reed*
Acheteur: *Sandy Ludovissy*
Coordonnatrice de conception: *Brenda A. Rolwes*
Couverture peinture: Jasper Johns, *Entre l'horloge et le lit*, 1981. Huile sur toile (72 × 126 1/ 4 pouces)
Collection de l'artiste. Photographie de Glenn Stiegelman. Couverture © Jasper Johns / sous licence VAGA, New York, NY
Concepteur de la couverture: *Studio Montage, St. Louis, Missouri*
Coordonnatrice principale de la recherche photo: *Carrie K. Burger*
Chef de projet média: *Tammy Juran*
Services de production / Compositeur: *RPK Editorial Services / PreTeX, Inc.*
Police de caractère: *10,5 / 12 fois romaine*
Imprimeur: *RR Donnelley*

Données de catalogage avant publication de la Bibliothèque du Congrès

Rosen, Kenneth H.
Mathématiques discrètes et leurs applications / Kenneth H. Rosen.- 7e éd.
p. cm.
Comprend un index.
ISBN 0–07–338309–0
1. Mathématiques. 2. Informatique - Mathématiques. I. Titre.
QA39.3.R67 2012
511 – dc22
2011011060

www.mhhe.com

Contenu

A propos de l'auteur

Kenneth H. Rosen a eu une longue carrière en tant que membre distingué du personnel technique aux laboratoires AT&T dans le comté de Monmouth, New Jersey. Il occupe actuellement le poste professeur invité à l'Université de Monmouth, où il enseigne des cours de troisième cycle en l'informatique.

Le Dr Rosen a obtenu son BS en mathématiques de l'Université du Michigan, Ann Arbor (1972), et son doctorat. en mathématiques du MIT (1976), où il a écrit sa thèse dans le domaine de la théorie des nombres sous la direction de Harold Stark. Avant de rejoindre Bell Laboratories en 1982, il a occupé des postes à l'Université du Colorado à Boulder; Université d'État de l'Ohio, Columbus; et l'Université du Maine, Orono, où il était professeur agrégé de mathématiques. Tout en travaillant à AT&T Labs, il a enseigné à l'Université de Monmouth, donnant des cours en mathématiques, théorie du codage et sécurité des données. Il enseigne actuellement des cours de conception d'algorithmes et en sécurité informatique et cryptographie.

Le Dr Rosen a publié de nombreux articles dans des revues professionnelles sur la théorie des nombres et en modélisation mathématique. Il est l'auteur de la *théorie des nombres élémentaires* largement utilisée *et Ses applications*, publiées par Pearson, actuellement dans sa sixième édition, qui a été traduite en chinois. Il est également l'auteur de *Discrete Mathematics and Its Applications*, publié par McGraw-Hill, actuellement dans sa septième édition. *Les mathématiques discrètes et leurs applications* ont vendu à plus de 350 000 exemplaires en Amérique du Nord au cours de sa vie, et des centaines de milliers de copies dans le reste du monde. Ce livre a également été traduit en espagnol, Français, grec, chinois, vietnamien et coréen. Il est également co-auteur d' *UNIX: The Complete Référence* ; *UNIX System V version 4: une introduction* ; et les *meilleurs conseils UNIX jamais* publiés par Osborne McGraw-Hill. Ces livres se sont vendus à plus de 150 000 exemplaires, avec des traductions en Chinois, allemand, espagnol et italien. Le Dr Rosen est également l'éditeur du *Handbook of Discrete and Combinatorial Mathematics*, publié par CRC Press, et il est le rédacteur en chef consultatif du Série de livres du CRC en mathématiques discrètes, composée de plus de 55 volumes sur différents aspects des mathématiques discrètes, dont la plupart sont présentés dans ce livre. Le Dr Rosen sert de Rédacteur en chef adjoint de la revue *Discrete Mathematics*, où il travaille avec des articles soumis en plusieurs domaines des mathématiques discrètes, y compris la théorie des graphes, l'énumération et la théorie des nombres. Il s'intéresse également à l'intégration de logiciels mathématiques dans l'enseignement et la formation professionnelle environnements, et a travaillé sur plusieurs projets avec le logiciel Maple TM de Waterloo Maple Inc. dans ces deux domaines. Le Dr Rosen a également travaillé avec plusieurs maisons d'édition sur leur plates-formes de livraison de devoirs.

Aux laboratoires Bell et AT&T, le Dr Rosen a travaillé sur un large éventail de projets, y compris des études de recherche opérationnelle, la planification de la gamme de produits pour les ordinateurs et la communication de données équipement de cations et évaluation de la technologie. Il a aidé à planifier les produits et services d'AT & T dans le domaine du multimédia, y compris les communications vidéo, la reconnaissance vocale, la synthèse vocale, et le réseautage d'images. Il a évalué les nouvelles technologies à utiliser par AT&T et a travaillé sur les normes dans le domaine du réseautage d'images. Il a également inventé de nombreux nouveaux services et détient plus de 55 brevets. Un de ses projets les plus intéressants consistait à aider à évaluer la technologie pour l'AT & T attraction qui faisait partie du Centre EPCOT.

Préface

En écrivant ce livre, j'ai été guidé par ma longue expérience et mon intérêt pour l'enseignement Mathématiques discrètes. Pour l'étudiant, mon but était de présenter du matériel de manière précise, manière lisible, avec les concepts et techniques des mathématiques discrètes clairement présentés et démontré. Mon objectif était de montrer la pertinence et le caractère pratique des mathématiques discrètes aux étudiants, qui sont souvent sceptiques. Je voulais donner aux étudiants qui étudient l'informatique tous les bases mathématiques dont ils ont besoin pour leurs études futures.Je voulais donner des mathématiques les élèves une compréhension des concepts mathématiques importants ainsi qu'un sens de pourquoi ces concepts sont importants pour les applications. Et surtout, je voulais accomplir ces objectifs sans diluer le matériau.

Pour l'instructeur, mon objectif était de concevoir un outil pédagogique flexible et complet utilisant techniques pédagogiques éprouvées en mathématiques. Je voulais fournir aux instructeurs un package de matériaux qu'ils pourraient utiliser pour enseigner les mathématiques discrètes de manière efficace et efficiente dans le manière la plus appropriée pour leur ensemble particulier d'élèves. J'espère avoir atteint ces buts.

J'ai été extrêmement satisfait de l'énorme succès de ce texte. Les nombreuses améliorations dans la septième édition ont été rendus possibles grâce aux commentaires et suggestions d'un grand nombre d'instructeurs et d'élèves dans plusieurs des plus de 600 écoles nord-américaines, et dans de nombreuses universités dans certaines parties du monde, où ce livre a été utilisé avec succès.

Ce texte est conçu pour un cours introductif de mathématiques discrètes d'un ou deux trimestres par des étudiants dans une grande variété de disciplines, y compris les mathématiques, l'informatique et ing. L'algèbre collégiale est la seule condition préalable explicite, bien qu'un certain degré de la maturité est nécessaire pour étudier les mathématiques discrètes de manière significative.Ce livre a été rédigé signé pour répondre aux besoins de presque tous les types de cours d'introduction aux mathématiques discrètesIl est très flexible et extrêmement complet. Le livre est conçu non seulement pour être un succès manuel, mais aussi pour servir de ressource précieuse que les étudiants peuvent consulter tout au long de leurs études et la vie professionnelle.

Objectifs d'un cours de mathématiques discrètes

Un cours de mathématiques discret a plus d'un objectif. Les étudiants devraient apprendre un ensemble de faits mathématiques et comment les appliquer;plus important encore, un tel cours devrait enseigner les élèves à penser de façon logique et mathématique.Pour atteindre ces objectifs, ce texte souligne le raisonnement mathématique et les différentes manières de résoudre les problèmes.Cinq thèmes importants sont entrelacés dans ce texte: raisonnement mathématique, analyse combinatoire, structures discrètes, pensée algorithmique, applications et modélisation. Un cours de mathématiques discrètes réussi devrait soigneusement mélanger et équilibrer les cinq thèmes.

1. *Raisonnement mathématique: les* élèves doivent comprendre le raisonnement mathématique pour lire, comprendre et construire des arguments mathématiques. Ce texte commence par une discussion de la logique mathématique, qui sert de base pour les discussions ultérieures de méthodes de preuve. La science et l'art de construire des preuves sont abordés.le la technique d'induction mathématique est soulignée à travers de nombreux types d'exemples de ces preuves et une explication minutieuse de la raison pour laquelle l'induction mathématique est une preuve valide technique.

2. *Analyse combinatoire:* une compétence importante en résolution de problèmes est la capacité de compter ou merate objets. La discussion de l'énumération dans ce livre commence par les techniques de base de compter. L'accent est mis sur la réalisation d'analyses combinatoires pour résoudre les problèmes de comptage et analyser des algorithmes, pas sur l'application de formules.
3. *Structures discrètes:* un cours de mathématiques discrètes devrait enseigner aux élèves comment travailler avec des structures discrètes, qui sont les structures mathématiques abstraites utilisées pour représenter objets discrets et relations entre ces objets. Ces structures discrètes comprennent ensembles, permutations, relations, graphiques, arbres et machines à états finis.
4. *Pensée algorithmique:* certaines classes de problèmes sont résolues par la spécification d'un algorithme. Après la description d'un algorithme, un programme informatique peut être construit sa mise en œuvre. Les parties mathématiques de cette activité, qui incluent la spécification de l'algorithme, la vérification de son bon fonctionnement et l'analyse de l'ordinateur mémoire et le temps nécessaire pour l'exécuter, sont tous couverts dans ce texte. Les algorithmes sont décrits en utilisant à la fois l'anglais et une forme de pseudocode facilement compréhensible.
5. *Applications et modélisation:* les mathématiques discrètes ont des applications dans presque toutes les conceptions. domaine d'étude. Il existe de nombreuses applications à l'informatique et aux réseaux de données dans ce texte, ainsi que des applications à des domaines aussi divers que la chimie, la biologie, la linguistique, géographie, commerce et Internet. Ces applications sont des utilisations naturelles et importantes de mathématiques discrètes et ne sont pas artificielles. La modélisation avec des mathématiques discrètes est un compétences de résolution de problèmes extrêmement importantes, que les élèves ont la possibilité de développer en construire leurs propres modèles dans certains des exercices.

Changements dans la septième édition

Bien que la sixième édition ait été un texte extrêmement efficace, de nombreux instructeurs, y compris les utilisateurs de longue date ont demandé des modifications destinées à rendre ce livre plus efficace.j'ai consacré beaucoup de temps et d'énergie pour satisfaire leurs demandes et j'ai travaillé dur pour trouver mes propres moyens de rendre le livre plus efficace et plus convaincant pour les étudiants.

La septième édition est une révision majeure, avec des changements basés sur les contributions de plus de 40 réviseurs formels, rétroaction des étudiants et des instructeurs et perspectives des auteurs.Le résultat est un nouvelle édition qui offre une meilleure organisation des sujets rendant le livre plus efficace outil pédagogique. Améliorations substantielles du matériel consacré à la logique, aux algorithmes, au nombre la théorie et la théorie des graphes rendent ce livre plus flexible et plus complet.De nombreux changements dans la septième édition ont été conçus pour aider les étudiants à apprendre plus facilement le matériel. Des explications et des exemples supplémentaires ont été ajoutés pour clarifier le matériel là où les étudiants Avoir de la difficulté. De nouveaux exercices, à la fois routiniers et stimulants, ont été ajoutés. Très pertinent applications, y compris de nombreuses applications liées à Internet, à l'informatique et aux mathématiques biologie, ont été ajoutés. Le site Web compagnon a bénéficié d'un vaste développement activité et fournit maintenant des outils que les élèves peuvent utiliser pour maîtriser les concepts clés et explorer le monde de mathématiques discrètes, et de nombreux nouveaux outils en cours de développement seront publiés dans l'année après la publication de ce livre.

J'espère que les instructeurs examineront attentivement cette nouvelle édition pour découvrir comment elle pourrait se rencontrer leurs besoins. Bien qu'il ne soit pas pratique d'énumérer tous les changements dans cette édition, une brève liste met en évidence certains changements clés, répertoriés par les avantages qu'ils procurent, peuvent être utiles.

Organisation plus flexible

- Les applications de la logique propositionnelle se trouvent dans une nouvelle section dédiée, qui introduit des circuits logiques.
- Les relations de récurrence sont maintenant traitées dans le chapitre 2.
- Une couverture étendue de la comptabilité est désormais disponible dans une section dédiée du chapitre 2.

- Des chapitres distincts offrent désormais une couverture étendue des algorithmes (chapitre 3) et du nombre théorie et cryptographie (chapitre 4).
- Plus de têtes de deuxième et troisième niveaux ont été utilisées pour diviser les sections en les pièces.

Outils pour un apprentissage plus facile

- Des discussions et des preuves difficiles ont été marquées par le fameux Bourbaki «dangereux plier "dans la marge.

- De nouvelles notes marginales établissent des liens, ajoutent des notes intéressantes et fournissent des étudiants.
- Plus de détails et d'explications supplémentaires, tant dans les épreuves que dans l'exposé, facilitent aux élèves de lire le livre.
- De nombreux nouveaux exercices, routiniers et stimulants, ont été ajoutés, tandis que de nombreux Les exercices existants ont été améliorés.

Couverture améliorée de la logique, des ensembles et de la preuve

- Le problème de satisfiabilité est traité plus en profondeur, avec Sudoku modélisé en termes de satisfiabilité.
- Hilbert's Grand Hotel est utilisé pour aider à expliquer le dénombrement.
- Les preuves tout au long du livre ont été rendues plus accessibles en ajoutant des étapes et des raisons derrière ces étapes.
- Un modèle de preuves par induction mathématique a été ajouté.
- L'étape qui applique l'hypothèse inductive dans la preuve d'induction mathématique est maintenant explicitement noté.

Des algorithmes

- Le pseudocode utilisé dans le livre a été mis à jour.
- Couverture explicite des paradigmes algorithmiques, y compris la force brute, les algorithmes cupides, et une programmation dynamique, est maintenant fournie.
- Les règles utiles pour les estimations de grand O des logarithmes, des puissances et des fonctions exponentielles ont ajouté.

Théorie des nombres et cryptographie

- Une couverture étendue permet aux instructeurs d'inclure juste un peu ou beaucoup de théorie des nombres dans leurs cours.
- La relation entre la fonction **mod** et les congruences a été expliquée plus pleinement.
- Le tamis d'Ératosthène est maintenant présenté plus tôt dans le livre.
- Les congruences linéaires et les inverses modulaires sont maintenant traités plus en détail.
- Les applications de la théorie des nombres, y compris les chiffres de contrôle et les fonctions de hachage, sont couvertes en profondeur.
- Une nouvelle section sur la cryptographie intègre la couverture précédente et la notion de cryptage tosystem a été introduit.
- Les protocoles cryptographiques, y compris les signatures numériques et le partage de clés, sont désormais couverts.

La théorie des graphes

- Une introduction structurée aux applications de la théorie des graphes a été ajoutée.
- Plus de couverture a été consacrée à la notion de réseaux sociaux.
- Applications aux sciences biologiques et applications motivantes pour l'isomor- phisme et planarité ont été ajoutés.
- Les correspondances dans les graphes bipartites sont désormais couvertes, y compris le théorème de Hall et sa preuve.
- La couverture de la connectivité des sommets, de la connectivité des bords et de la n- connectivité a été ajouté, fournissant plus de renseignements sur la connectivité des graphiques.

Matériel d'enrichissement

- De nombreuses biographies ont été développées et mises à jour, et de nouvelles biographies de Bellman, Bézout Bienyamé, Cardano, Catalan, Cocks, Cook, Dirac, Hall, Hilbert, Ore et Tao ont été ajoutés.
- Des informations historiques ont été ajoutées tout au long du texte.
- De nombreuses mises à jour des dernières découvertes ont été effectuées.

Médias étendus

- Des efforts considérables ont été consacrés à la production de précieuses ressources Web pour ce livre.
- Des exemples supplémentaires dans des parties clés du texte ont été fournis sur le site Web complémentaire.
- Des algorithmes interactifs ont été développés, avec des outils pour les utiliser pour explorer des sujets et pour une utilisation en classe.
- Un nouvel accessoire en ligne, *The Virtual Discrete Mathematics Tutor* , disponible à l'automne 2012, aidera les élèves à surmonter les problèmes d'apprentissage des mathématiques discrètes.
- Un nouveau système de livraison de devoirs, disponible à l'automne 2012, fournira des travailler pour des exercices numériques et conceptuels.
- Des modules d'évaluation des élèves sont disponibles pour les concepts clés.
- Des transparents PowerPoint pour les instructeurs ont été développés.
- Un supplément *Exploring Discrete Mathematics* a été développé, fournissant des informations prise en charge de l'utilisation de MapleTM ou Mathematica TM conjointement avec le livre.
- Une vaste collection de liens Web externes est fournie.

Caractéristiques du livre

ACCESSIBILITÉ Ce texte s'est avéré facile à lire et à comprendre en commençant étudiants. Il n'y a pas de prérequis mathématiques au-delà de l'algèbre universitaire pour presque tous les contenu du texte. Les étudiants ayant besoin d'une aide supplémentaire trouveront des outils sur le site Web amenant leur maturité mathématique au niveau du texte. Les quelques endroits du livre où le calcul est mentionné sont explicitement indiqués. La plupart des étudiants devraient facilement comprendre pseudocode utilisé dans le texte pour exprimer des algorithmes, qu'ils aient ou non formellement étudié les langages de programmation. Il n'y a pas de pré-requis informatique formel.

Chaque chapitre commence à un niveau facilement compréhensible et accessible. Une fois mathématique de base des concepts ont été soigneusement développés, des matériaux plus difficiles et des applications à d'autres domaines d'études sont présentés.

LA FLEXIBILITÉ Ce texte a été soigneusement conçu pour une utilisation flexible. La dépendance des chapitres sur le matériel précédent a été minimisé. Chaque chapitre est divisé en sections de environ la même longueur, et chaque section est divisée en sous-sections qui forment des blocs de matériel pour l'enseignement. Les instructeurs peuvent facilement rythmer leurs cours en utilisant ces blocs.

STYLE D'ÉCRITURE Le style d'écriture de ce livre est direct et pragmatique. Matière précise le langage matique est utilisé sans formalisme ni abstraction excessifs. On a pris soin de équilibrer le mélange de notation et de mots dans les énoncés mathématiques.

RIGUEUR MATHÉMATIQUE ET PRÉCISION Toutes les définitions et théorèmes de ce texte sont énoncées avec beaucoup de soin afin que les élèves puissent apprécier la précision de la langue et rigueur nécessaire en mathématiques. Les preuves sont motivées et développées lentement; leurs pas sont tous soigneusement justifié. Les axiomes utilisés dans les preuves et les propriétés de base qui en découlent sont explicitement décrits dans une annexe, donnant aux élèves une idée claire de ce qu'ils peuvent une preuve. Les définitions récursives sont expliquées et largement utilisées.

EXEMPLES TRAVAILLÉS Plus de 800 exemples sont utilisés pour illustrer des concepts, relier différents et présenter des applications. Dans la plupart des exemples, une question est d'abord posée, puis sa solution est présenté avec la quantité appropriée de détails.

APPLICATIONS Les applications incluses dans ce texte démontrent l'utilité de mathématiques dans la solution de problèmes du monde réel. Ce texte comprend des applications à un large éventail de de nombreux domaines, dont l'informatique, le réseautage de données, la psychologie, la chimie, l'ingénierie, linguistique, biologie, commerce et Internet.

ALGORITHMES Les résultats en mathématiques discrètes sont souvent exprimés en termes d'algo-rithms; par conséquent, des algorithmes clés sont introduits dans chaque chapitre du livre. Ces algorithmes sont exprimés en mots et sous une forme facilement compréhensible de pseudocode structuré, qui est décrites et spécifiées à l'annexe 3. La complexité de calcul des algorithmes dans le texte est également analysé au niveau élémentaire.

INFORMATION HISTORIQUE Le contexte de nombreux sujets est succinctement décrit dans le texte. De brèves biographies de 83 mathématiciens et informaticiens sont incluses Remarques. Ces biographies contiennent des informations sur la vie, la carrière et les réalisations de ces contributeurs importants aux mathématiques et images discrètes, lorsqu'ils sont disponibles, sont affichés.

De plus, de nombreuses notes de bas de page historiques sont incluses qui complètent formation dans le corps du texte. Des efforts ont été faits pour maintenir le livre à jour en reflétant les dernières découvertes.

TERMES ET RÉSULTATS CLÉS Une liste de termes et de résultats clés suit chaque chapitre.le les termes clés incluent uniquement les plus importants que les élèves doivent apprendre, et non tous les termes définis dans le chapitre.

DES EXERCICES Il y a plus de 4000 exercices dans le texte, avec de nombreux types différents de questions posées. Il existe une multitude d'exercices simples qui développent les compétences de base, un grand nombre d'exercices intermédiaires et de nombreux exercices difficiles.Les exercices sont énoncés clairement et sans ambiguïté, et tous sont soigneusement classés pour le niveau de difficulté.Ensembles d'exercices contiennent des discussions spéciales qui développent de nouveaux concepts non couverts dans le texte, permettant aux étudiants découvrir de nouvelles idées à travers leur propre travail.

Les exercices un peu plus difficiles que la moyenne sont marqués d'une seule étoile *; ceux qui sont beaucoup plus difficiles sont marqués de deux étoiles **. Des exercices dont les solutions nécessitent un calcul sont explicitement notés. Les exercices qui développent les résultats utilisés dans le texte sont clairement identifié avec le symbole de la main pointée vers la droite . Réponses ou solutions esquissées à toutes les

des exercices numérotés sont fournis à la fin du texte.Les solutions comprennent des preuves dans lesquelles la plupart des étapes sont clairement énoncées.

RÉVISION DES QUESTIONS Un ensemble de questions de révision est fourni à la fin de chaque chapitre. Ces questions sont conçues pour aider les étudiants à concentrer leur étude sur les concepts les plus importants et les techniques de ce chapitre. Pour répondre à ces questions, les élèves doivent écrire de longues réponses, plutôt que de simplement effectuer des calculs ou de donner de courtes réponses.

ENSEMBLES D'EXERCICES SUPPLÉMENTAIRES Chaque chapitre est suivi d'un livre riche et varié ensemble d'exercices supplémentaires. Ces exercices sont généralement plus difficiles que ceux du ensembles d'exercices suivant les sections. Les exercices supplémentaires renforcent les concepts de la chapitre et intégrer plus efficacement différents sujets.

PROJETS INFORMATIQUES Chaque chapitre est suivi d'un ensemble de projets informatiques.le environ 150 projets informatiques relient ce que les élèves peuvent avoir appris en informatique et en mathématiques discrètes. Projets informatiques plus difficiles que la moyenne, des deux d'un point de vue mathématique et de programmation, sont marqués d'une étoile, et ceux qui sont extrêmement difficile sont marqués de deux étoiles.

CALCULS ET EXPLORATIONS Un ensemble de calculs et d'explorations est inclus à la fin de chaque chapitre.Ces exercices (environ 120 au total) sont signé pour être complété à l'aide d'outils logiciels existants, tels que des programmes que les étudiants ou teurs ont des progiciels de calcul écrit ou mathématique tels que MapleTM ou Mathematica TM . Bon nombre de ces exercices donnent aux élèves l'occasion de découvrir de nouveaux faits et idées calcul. (Certains de ces exercices sont abordés dans la section *Exploration des mathématiques discrètes* cahiers d'exercices complémentaires disponibles en ligne.)

PROJETS D'ÉCRITURE Chaque chapitre est suivi d'un ensemble de projets d'écriture.Pour faire ça projets les élèves doivent consulter la littérature mathématique.Certains de ces projets sont historiques dans la nature et peut impliquer la recherche de sources originales.D'autres sont conçus pour servir de passerelles à de nouveaux sujets et idées. Tous sont conçus pour exposer les étudiants à des idées non couvertes en profondeur dans le texte. Ces projets associent des concepts mathématiques au processus d'écriture et aident exposer les élèves à des domaines possibles pour de futures études.(Les références suggérées pour ces projets peuvent se trouve en ligne ou dans le *Guide des solutions pour les étudiants* .)

APPENDICES Il y a trois annexes au texte. Le premier introduit des axiomes pour de vrai les nombres et les nombres entiers positifs, et illustre comment les faits sont prouvés directement à partir de ces axiomes. Le second couvre les fonctions exponentielles et logarithmiques, en passant en revue certains matériaux de base utilisés fortement dans le cours. Le troisième précise le pseudocode utilisé pour décrire les algorithmes dans ce texte.

LECTURES SUGGÉRÉES Une liste de lectures suggérées pour l'ensemble du livre et pour chaque chapitre est fourni après les annexes.Ces lectures suggérées comprennent des livres à ou au-dessous le niveau de ce texte, des livres plus difficiles, des articles d'exposition et des articles dans lesquels des découvertes en mathématiques discrètes ont été initialement publiés.Certaines de ces publications sont des classiques, publié il y a de nombreuses années, tandis que d'autres ont été publiés ces dernières années.

Comment utiliser ce livre

Ce texte a été soigneusement rédigé et construit pour soutenir des cours de mathématiques discrets à plusieurs niveaux et avec des foyers différents. Le tableau suivant identifie le noyau et facultatif sections. Un cours d'introduction à un trimestre en mathématiques discrètes au niveau de la deuxième année peut être basé sur les sections principales du texte, les autres sections étant couvertes à la discrétion du

instructeur. Un cours d'introduction de deux trimestres peut inclure toutes les sections optionnelles de mathématiques en plus des sections centrales. Un cours avec un fort accent informatique peut être enseigné en couvrant une partie ou la totalité des sections facultatives en informatique. Les instructeurs peuvent trouver un échantillon programmes pour un large éventail de cours de mathématiques discrets et des suggestions d'enseignement pour chaque utilisation section du texte peut être trouvée dans le *Guide de ressources de* l' *instructeur* disponible sur le site Web pour ce livre.

Chapitre	*Coeur*	*CS en option*	*Math optionnel*
1	1.1–1.8 (au besoin)		
2	2.1–2.4, 2.6 (au besoin)		2,5
3		3.1–3.3 (au besoin)	
4	4.1–4.4 (au besoin)	4.5, 4.6	
5	5.1–5.3	5.4, 5.5	
6	6.1–6.3	6,6	6.4, 6.5
sept	7.1	7.4	7.2, 7.3
8	8.1, 8.5	8.3	8.2, 8.4, 8.6
9	9.1, 9.3, 9.5	9.2	9.4, 9.6
dix	10.1–10.5		10,6–10,8
11	11.1	11.2, 11.3	11.4, 11.5
12		12,1–12,4	
13		13,1–13,5	

Les instructeurs utilisant ce livre peuvent ajuster le niveau de difficulté de leur cours en choisissant soit pour couvrir ou pour omettre les exemples les plus difficiles à la fin des sections, ainsi que les exercices les plus difficiles. Le tableau de dépendance des chapitres montré ici montre la forte dépendances. Une étoile indique que seules les sections pertinentes du chapitre sont nécessaires pour étudier un chapitre ultérieur. Les dépendances faibles ont été ignorées. Plus de détails peuvent être trouvés dans l'instructeur Guide de ressources.

Chapitre 1
Chapitre 2*
Chapitre 12
Chapitre 3*
Chapitre 9 *
Chapitre 4*
Chapitre 10 *
Chapitre 13
Chapitre 5*
Chapitre 11
Chapitre 6*
Chapitre 7
Chapitre 8

Auxiliaires

GUIDE DES SOLUTIONS DES ÉTUDIANTS Ce manuel de l'étudiant, disponible séparément, contient des solutions complètes à tous les problèmes impairs dans les ensembles d'exercices. Ces solutions expliquent pourquoi une méthode particulière est utilisée et pourquoi elle fonctionne. Pour certains exercices, un ou deux autres possibles Des approches sont décrites pour montrer qu'un problème peut être résolu de plusieurs manières différentes. Sug- les références pour les projets d'écriture qui se trouvent à la fin de chaque chapitre sont également ce volume. Sont également inclus un guide pour la rédaction des épreuves et une description détaillée des les erreurs que les élèves font en mathématiques discrètes, ainsi que des exemples de tests et un exemple de feuille de chaque chapitre est conçu pour aider les étudiants à se préparer aux examens.

(ISBN-10: 0-07-735350-1) *(ISBN-13: 978-0-07-735350-6)*

GUIDE DES RESSOURCES DE L'INSTRUCTEUR Ce manuel, disponible sur le site Internet et en formulaire imprimé sur demande pour les instructeurs, contient des solutions complètes aux exercices pairs le texte. Des suggestions sur la façon d'enseigner le matériel dans chaque chapitre du livre sont fournies, y compris les points à souligner dans chaque section et comment mettre le matériel en perspective.Il propose également des exemples de tests pour chaque chapitre et une banque de tests contenant plus de 1500 questions d'examen à choisissez parmi. Les réponses à tous les exemples de tests et aux questions sur les banques de tests sont incluses.Enfin, plusieurs des exemples de programmes sont présentés pour les cours avec des accents différents et des niveaux de capacité des étudiants.

(ISBN-10: 0-07-735349-8) *(ISBN-13: 978-0-07-735349-0)*

Remerciements

Je voudrais remercier les nombreux instructeurs et étudiants de diverses écoles qui ont utilisé ce livre et m'a fourni leurs précieux commentaires et suggestions utiles.Leur contribution a fait de ce livre un bien meilleur livre qu'il ne l'aurait été autrement.Je veux surtout remercier Jerrold Grossman, Jean-Claude Evard et Georgia Mederer pour leurs revues techniques du septième édition et leurs «yeux d'aigle», qui ont contribué à assurer l'exactitude de ce livre.je apprécions également l'aide fournie par tous ceux qui ont soumis des commentaires via le site Web.

Je remercie les critiques de cette septième et des six éditions précédentes.Ces examinateurs ont m'a fourni des critiques et des encouragements très utiles.J'espère que cette édition sera à la hauteur de leur des attentes élevées.

Relecteurs pour la septième édition

Philip Barry
Université du Minnesota, Minneapolis

Miklos Bona
Université de Floride

Kirby Brown
Queens College

John Carter
Université de Toronto

Narendra Chaudhari
Université technologique de Nanyang

Allan Cochran
Université d'Arkansas

Daniel Cunningham
Buffalo State College

George Davis
Université d'État de Géorgie

Andrzej Derdzinski
Université d'État de l'Ohio

Ronald Dotzel
Université du Missouri-St. Louis

TJ Duda
Columbus State Community College

Bruce Elenbogen
Université du Michigan, Dearborn

Norma Elias
Université Purdue, Calumet-Hammond

Herbert Enderton
Université de Californie, Los Angeles

Anthony Evans
Université d'État de Wright

Facteur Kim
Université Marquette

Margaret Fleck
Université de l'Illinois, Champaign

Peter Gillespie
Université d'État de Fayetteville

Johannes Hattingh
Université d'État de Géorgie

Ken Holladay
Université de la Nouvelle-Orléans

Jerry Ianni
Collège communautaire LaGuardia

Ravi Janardan
Université du Minnesota, Minneapolis

Norliza Katuk
Université d'Utara en Malaisie

William Klostermeyer
Université de Floride du Nord

Przemo Kranz
Université du Mississippi

Jaromy Kuhl
Université de Floride occidentale

Loredana Lanzani
Université de l'Arkansas, Fayetteville

Steven Leonhardi
Université d'État de Winona

Xu Liutong
Université des postes de Pékin et Télécommunications

Vladimir Logvinenko
De Anza Community College

Darrell Minor
Columbus State Community College

Keith Olson
Université d'Utah Valley

Yongyuth Permpoontanalarp
Université du Roi Mongkut Technologie, Thonburi

Galin Piatniskaia
Université du Missouri, St. Louis

Stefan Robila
Université d'État de Montclair

Chris Rodger
Université d'Auburn

Sukhit Singh
Université d'État du Texas, San Marcos

David Snyder
Université d'État du Texas, San Marcos

Wasin So
Université d'État de San Jose

Bogdan Suceava
Université d'État de Californie, Fullerton

Christopher Swanson
Université d'Ashland

Bon Sy
Queens College

Matthew Walsh
Université Indiana-Purdue, Fort Wayne

Gideon Weinstein
Université Western Governors

David Wilczynski
Université de Californie du Sud

Je tiens à remercier Bill Stenquist, rédacteur en chef, pour son plaidoyer, son enthousiasme et soutien. Son aide pour cette édition a été essentielle. Je remercie également l'original éditeur, Wayne Yuhasz, dont les idées et les compétences ont contribué à assurer le succès du livre, ainsi que tous les nombreux autres éditeurs précédents de ce livre.

Je tiens à exprimer ma reconnaissance au personnel des services éditoriaux de RPK pour leur travailler sur cette édition, y compris Rose Kernan, qui a été à la fois le rédacteur en chef du développement et l'éditeur de production et les autres membres de l'équipe du RPK, Fred Dahl, Martha McMaster, Erin Wagner, Harlan James et Shelly Gerger-Knecthl. Je remercie Paul Mailhot de PreTeX, Inc., le compositeur, pour l'énorme travail qu'il a consacré à la réalisation de cette édition, et pour sa connaissance intime de LaTeX. Merci également à Danny Meldung de Photo Affairs, Inc., qui a été ingénieux en obtenant des images pour les nouvelles notes biographiques.

La précision et la qualité de cette nouvelle édition doivent beaucoup à Jerry Grossman et Jean-Claude Evard, qui a vérifié l'intégralité du manuscrit pour l'exactitude technique et Georgia Mederer, qui vérifié l'exactitude des réponses à la fin du livre et des solutions dans les *années des étudiants Guide de solutions* et *guide de ressources de l'instructeur* . Comme d'habitude, je ne peux pas remercier Jerry Grossman assez pour tout son travail auteur de ces deux auxiliaires essentiels.

Je voudrais également exprimer ma gratitude pour les sciences, l'ingénierie et les mathématiques (SEM) Division of McGraw-Hill Higher Education pour leur précieux soutien à cette nouvelle édition et le contenu multimédia associé. En particulier, merci à Kurt Strand: président, SEM, McGraw-Hill Higher Education, Marty Lange: rédacteur en chef, SEM, Michael Lange: directeur éditorial, Raghothaman Srinivasan: éditeur mondial, Bill Stenquist: rédacteur en chef, Curt Reynolds: Directrice Marketing Exécutive, Robin A. Reed: Chef de Projet, Sandy Ludovissey: Acheteur, Lorraine Buczek: rédactrice en chef du développement, Brenda Rowles: coordonnatrice de la conception, Carrie K. Burger: coordonnatrice principale de la recherche photo et Tammy Juran: gestionnaire de projet média.

Kenneth H. Rosen

Le site Web du compagnon

Le vaste site Web d'accompagnement accompagnant ce texte a été considérablement amélioré pour la septième édition Ce site Web est accessible à l'*adresse www.mhhe.com/rosen* . La page d'accueil affiche le *centre de documentation* et contient des liens de connexion pour le site*étudiant* et l' *instructeur du site Site* . Les principales caractéristiques de chaque domaine sont décrites ci-dessous:

LE CENTRE D'INFORMATION

Le centre d'information contient des informations de base sur le livre, y compris le table des matières (y compris les titres des sous-sections), la préface, la description des accessoires et un exemple de chapitre. Il fournit également un lien qui peut être utilisé pour soumettre des rapports d'errata et d'autres commentaires sur le livre.

SITE ÉTUDIANT

Le site étudiant contient une multitude de ressources disponibles pour les étudiants, y compris le ci-dessous, liés au texte partout où les icônes spéciales affichées ci-dessous se trouvent dans le texte:

- ***Exemples supplémentaires*** Vous pouvez trouver un grand nombre d'exemples supplémentaires sur le site, couvrant tous les chapitres du livre. Ces exemples sont concentrés dans des domaines où les étudiants demandez du matériel supplémentaire. Bien que la plupart de ces exemples amplifient les concepts de base, des exemples plus difficiles peuvent également être trouvés ici.
- ***Applets de démonstration interactifs*** Ces applets vous permettent d'explorer de manière interactive l'importance des algorithmes et sont directement liés au contenu du texte avec des liens vers exemples et exercices. Des ressources supplémentaires sont fournies sur la façon d'utiliser et d'appliquer ces applets.
- ***Auto-évaluations*** Ces guides interactifs vous aident à évaluer votre compréhension de 14 clés concepts, fournissant une banque de questions où chaque question comprend un bref tutoriel suivi par une question à choix multiples. Si vous sélectionnez une réponse incorrecte, des conseils sont fournis pour vous aider vous comprenez votre erreur. En utilisant ces auto-évaluations, vous devriez pouvoir diagnostiquer vos problèmes et trouver l'aide appropriée.
- ***Guide des ressources Web*** Ce guide fournit des liens annotés vers des centaines de sites Web externes contenant des éléments pertinents tels que des informations historiques et biographiques, des puzzles et problèmes, discussions, applets, programmes, etc. Ces liens sont saisis vers le texte par page nombre.

Les ressources supplémentaires du site étudiant incluent:

- ***Exploration des mathématiques discrètes*** Cet accessoire fournit de l'aide pour utiliser une algè- système de soutien-gorge pour effectuer un large éventail de calculs en mathématiques discrètes. Chaque chapitre fournit une description des fonctions pertinentes du système d'algèbre informatique et de leur utilisation, grammes pour effectuer des calculs en mathématiques discrètes, des exemples et des exercices qui peuvent être travaillé en utilisant ce système d'algèbre informatique. Deux versions, *Exploring Discrete Mathematics avec Maple* TM et *Exploration des mathématiques discrètes avec Mathematica* TM seront disponibles.
- ***Applications des mathématiques discrètes*** Cet accessoire contient 24 chapitres, chacun avec sa propre série d'exercices - présentant une grande variété d'applications intéressantes et importantes

couvrant trois domaines généraux en mathématiques discrètes: les structures discrètes, la combinatoire et la théorie des graphes. Ces applications sont idéales pour compléter le texte ou pour une étude indépendante.

- ***A Guide to Proof-Writing*** Ce guide fournit une aide supplémentaire pour la rédaction d'épreuves, une compétence que de nombreux étudiants ont du mal à maîtriser. En lisant ce guide au début du cours et périodiquement par la suite lorsque la rédaction de preuves est requise, vous serez récompensé votre capacité de correction d'épreuves augmente. (Également disponible dans le *Student's Solutions Guide* .)

- ***Erreurs courantes en mathématiques discrètes*** Ce guide comprend une liste détaillée des les idées fausses que les élèves de mathématiques discrètes ont souvent et les types d'erreurs ils ont tendance à faire. Nous vous encourageons à consulter cette liste de temps en temps pour éviter ces pièges communs. (Également disponible dans le *Student's Solutions Guide* .)
- ***Conseils sur la rédaction de projets*** Ce guide offre des conseils et des suggestions utiles pour la rédaction Projets dans le texte, y compris une bibliographie complète d'ouvrages et d'articles utiles pour recherche; discussion de diverses ressources disponibles sur papier et en ligne;conseils sur la bibliothèque recherche; et des suggestions sur la façon de bien écrire.(Également disponible dans les *solutions étudiantes Guide* .)
- ***Le tuteur virtuel en mathématiques discrètes*** Ce vaste programme auxiliaire offre aux élèves une aide précieuse dans la transition des cours de niveau inférieur aux cours de mathématiques ics. Les erreurs que les élèves ont commises en étudiant des mathématiques discrètes à l'aide de ce texte ont été analysé pour concevoir cette ressource. Les étudiants pourront obtenir de nombreuses réponses à leurs questions et peut surmonter de nombreux obstacles via ces accessoires. Le *tuteur virtuel en mathématiques discrètes* devrait être disponible à l'automne 2012.

SITE DE L'INSTRUCTEUR

Cette partie du site Web donne accès à toutes les ressources du site étudiant, ainsi qu'aux ces ressources pour les instructeurs:

- ***Syllabi suggéré*** Des plans de cours détaillés sont affichés, offrant des suggestions de cours avec des accents différents et des antécédents et des niveaux de capacité différents.
- ***Suggestions pédagogiques*** Ce guide contient des suggestions pédagogiques détaillées pour les instructeurs, y compris des aperçus de chapitre pour le texte entier, des remarques détaillées sur chaque section et des commentaires sur les ensembles d'exercices.
- ***Tests*** imprimables Des tests imprimables sont proposés au format TeX et Word pour chaque chapitre, et peut être personnalisé par des instructeurs.
- ***Diapositives et tableaux PowerPoint PowerPoints*** Une vaste collection des diapositives PowerPoint pour tous les chapitres du texte sont fournies aux instructeurs. En plus, des images de toutes les figures et tableaux du texte sont fournies sous forme de diapositives PowerPoint.
- ***Système de livraison de devoirs*** Un ***système*** complet de livraison de devoirs, en cours de développement pour disponibilité à l'automne 2012, fournira des questions directement liées au texte, afin que les élèves sera en mesure de faire des affectations en ligne. De plus, ils pourront utiliser ce système dans un mode tutoriel. Ce système sera en mesure de classer automatiquement les affectations et de fournir former les étudiants aux instructeurs pour leur propre analyse. Les capacités de gestion des cours être fourni qui permettra aux instructeurs de créer des affectations, d'assigner automatiquement et de noter devoirs, quiz et testez des questions à partir d'une banque de questions directement liées au texte, créez et modifier leurs propres questions, gérer les annonces de cours et les dates d'échéance, et suivre les étudiants le progrès.

À l'étudiant

W *chapeau est les mathématiques discrètes?* Les mathématiques discrètes sont la partie des mathématiques consacrée à l'étude d'objets discrets. (Ici, *des* moyens *discrets* consistant en des éléments distincts ou non connectés éléments.) Les types de problèmes résolus en utilisant des mathématiques discrètes comprennent:

- De combien de façons existe-t-il pour choisir un mot de passe valide sur un système informatique?
- Quelle est la probabilité de gagner à une loterie?
- Y a-t-il un lien entre deux ordinateurs d'un réseau?
- Comment identifier les courriers électroniques indésirables?
- Comment puis-je crypter un message afin qu'aucun destinataire non prévu ne puisse le lire?
- Quel est le chemin le plus court entre deux villes utilisant un système de transport?
- Comment une liste d'entiers peut-elle être triée afin que les entiers soient dans l'ordre croissant?
- Combien d'étapes sont nécessaires pour effectuer un tel tri?
- Comment prouver qu'un algorithme de tri trie correctement une liste?

- Comment concevoir un circuit qui ajoute deux entiers?
- Combien y a-t-il d'adresses Internet valides?

Vous apprendrez les structures et les techniques discrètes nécessaires pour résoudre de tels problèmes.

Plus généralement, les mathématiques discrètes sont utilisées chaque fois que des objets sont comptés, les navires entre ensembles finis (ou dénombrables) sont étudiés, et lorsque des processus impliquant un nombre fini des étapes sont analysées. Une des principales raisons de l'augmentation de l'importance des mathématiques discrètes est ces informations sont stockées et manipulées par des machines informatiques de manière discrète.

POURQUOI ÉTUDIER LES MATHÉMATIQUES DISCRETES? Il existe plusieurs raisons importantes étudier les mathématiques discrètes. Tout d'abord, grâce à ce cours, vous pouvez développer votre maturité: c'est-à-dire votre capacité à comprendre et à créer des arguments mathématiques. Vous n'obtiendrez pas très loin dans vos études en sciences mathématiques sans ces compétences.

Deuxièmement, les mathématiques discrètes sont la porte d'entrée vers des cours plus avancés dans les sciences mathématiques. Les mathématiques discrètes fournissent les fondements mathématiques de nombreux cours d'informatique, y compris les structures de données, les algorithmes, la théorie des bases de données, les automates théorie, langages formels, théorie du compilateur, sécurité informatique et systèmes d'exploitation. Étudiants trouvent ces cours beaucoup plus difficiles quand ils n'ont pas eu les mathématiques appropriées fondements de mathématiques discrètes. Une étudiante m'a envoyé un e-mail me disant qu'elle utilisé le contenu de ce livre dans tous les cours d'informatique qu'elle a suivis!

Les cours de mathématiques basés sur le matériel étudié en mathématiques discrètes comprennent la logique, la théorie des ensembles, théorie des nombres, algèbre linéaire, algèbre abstraite, combinatoire, théorie des graphes et probabilité théorie (la partie discrète du sujet).

En outre, les mathématiques discrètes contiennent le fond mathématique nécessaire pour résoudre problèmes de recherche opérationnelle (y compris de nombreuses techniques d'optimisation discrètes), de chimie, ingénierie, biologie, etc. Dans le texte, nous étudierons les applications à certains de ces domaines.

De nombreux étudiants trouvent que leur cours d'introduction en mathématiques discrètes est beaucoup plus difficile que les cours qu'ils ont suivis auparavant. L'une des raisons à cela est que l'un des Les principaux objectifs de ce cours sont d'enseigner le raisonnement mathématique et la résolution de problèmes, plutôt qu'un ensemble discret de compétences. Les exercices de ce livre sont conçus pour refléter cet objectif. Bien que il y a beaucoup d'exercices dans ce texte similaires à ceux abordés dans les exemples, un grand

pourcentage des exercices nécessite une réflexion originale. C'est intentionnel. Le matériel discuté dans le texte fournit les outils nécessaires pour résoudre ces exercices, mais votre travail consiste à réussir appliquez ces outils en utilisant votre propre créativité. L'un des principaux objectifs de ce cours est d'apprendre comment attaquer des problèmes qui peuvent être quelque peu différents de ceux que vous pourriez avoir précédemment vu. Malheureusement, apprendre à résoudre uniquement certains types d'exercices n'est pas suffisant pour succès dans le développement des compétences en résolution de problèmes nécessaires dans les cours et les travail. Ce texte aborde de nombreux sujets différents, mais les mathématiques discrètes sont extrêmement diverses et vaste domaine d'étude. L'un de mes objectifs en tant qu'auteur est de vous aider à développer les compétences nécessaires pour maîtriser le matériel supplémentaire dont vous aurez besoin dans vos propres activités futures.

LES EXERCICES Je voudrais offrir quelques conseils sur la meilleure façon d'apprendre discrètement mathématiques (et d'autres matières dans les sciences mathématiques et informatiques). Vous apprendrez les la plupart en travaillant activement. Je vous suggère d'en résoudre autant que possible. Après en travaillant les exercices que votre instructeur vous a assignés, je vous encourage à résoudre des exercices supplémentaires telles que celles des jeux d'exercices qui suivent chaque section du texte et des annexes exercices à la fin de chaque chapitre. (Notez la clé expliquant les inscriptions précédant les exercices.)

Clé des exercices

pas de marquage	Un exercice de routine
*	Un exercice difficile
**	Un exercice extrêmement difficile
	Un exercice contenant un résultat utilisé dans le livre (Tableau 1 sur le la page suivante montre où ces exercices sont utilisés.)
(*Nécessite un calcul*)	Un exercice dont la solution nécessite l'utilisation de limites ou de concepts à partir du calcul différentiel ou intégral

La meilleure approche consiste à essayer vous-même les exercices avant de consulter la section des réponses fin de ce livre. Notez que les réponses aux exercices impaires fournies dans le texte sont des réponses solutions uniques et non complètes; en particulier, le raisonnement requis pour obtenir des réponses est omis dans ces réponses. Le *Guide des solutions aux étudiants* , disponible séparément, fournit des des solutions à tous les exercices impairs de ce texte. Lorsque vous sortez d'une impasse en essayant de résoudre un exercice impair, je vous suggère de consulter le *Guide des solutions pour* les *étudiants* et de chercher des conseils sur la façon de résoudre le problème. Plus vous travaillez vous-même plutôt que passivement en lisant ou en copiant des solutions, plus vous en apprendrez. Les réponses et les solutions à l'événement les exercices numérotés ne sont pas intentionnellement disponibles auprès de l'éditeur;demandez à votre instructeur si vous avoir des problèmes avec ceux-ci.

RESSOURCES WEB Vous êtes ***fortement*** encouragé à profiter de sources disponibles sur le Web, en particulier celles sur le site Web compagnon de ce livre trouvé sur *www.mhhe.com/rosen* . Vous trouverez de nombreux exemples supplémentaires conçus pour clarifier les concepts clés; Auto-évaluations pour évaluer dans quelle mesure vous comprenez les sujets essentiels; Démonstration interactive Applets explorant les algorithmes clés et d'autres concepts;un guide de ressources Web contenant un vaste sélection de liens vers des sites externes pertinents pour le monde des mathématiques discrètes;supplémentaire explications et pratique pour vous aider à maîtriser les concepts de base;instruction supplémentaire sur la rédaction des épreuves et éviter les erreurs courantes en mathématiques discrètes; des discussions approfondies sur les applications; et des conseils sur l'utilisation du logiciel Maple TM pour explorer les aspects informatiques des mathématiques discrètes. Emplacements dans le texte où ces ressources en ligne supplémentaires sont disponibles sont identifiés dans les marges par des icônes spéciales. Vous trouverez également (après l'automne 2012) le *Virtual Discrete Mathematics Tutor* , une ressource en ligne qui fournit un soutien supplémentaire pour vous aider à faire la transition des cours de niveau inférieur aux mathématiques discrètes. Ce tutoriel devrait aider à répondre bon nombre de vos questions et corriger les erreurs que vous pouvez faire, en fonction des erreurs d'autres élèves en utilisant ce livre, ont fait. Pour plus de détails sur ces ressources et d'autres ressources en ligne, consultez le description du site Web compagnon précédant immédiatement ce message «À l'étudiant».

TABLEAU 1 **Exercices sur les icônes de la main et où ils sont utilisés**

Section	*Exercice*	*Section où utilisé*	*Pages utilisées*
1.1	40	1,3	31
1.1	41	1,3	31
1,3	9	1,6	71
1,3	dix	1,6	70, 71
1,3	15	1,6	71
1,3	30	1,6	71, 74
1,3	42	12,2	820
1,7	16	1,7	86
2.3	72	2.3	144
2.3	79	2,5	170
2,5	15	2,5	174
2,5	16	2,5	173
3.1	43	3.1	197
3.2	72	11,2	761
4.2	36	4.2	270
4.3	37	4.1	239
4.4	2	4.6	301
4.4	44	7.2	464
6,4	17	7.2	466
6,4	21	7.4	480
7.2	15	7.2	466
9.1	26	9.4	598
10,4	59	11.1	747
11.1	15	11.1	750
11.1	30	11.1	755
11.1	48	11,2	762
12,1	12	12,3	825
A.2	4	8.3	531

LA VALEUR DE CE LIVRE Mon intention est de faire votre investissement substantiel dans ce texte d'une excellente valeur. Le livre, les accessoires associés et le site Web associé ont il a fallu de nombreuses années d'efforts pour développer et affiner.Je suis convaincu que la plupart d'entre vous le texte et les matériaux associés vous aideront à maîtriser les mathématiques discrètes, tout comme tant d'autres les étudiants précédents ont. Même s'il est probable que vous ne couvrirez pas certains chapitres de votre cours actuel, vous devriez trouver utile, comme beaucoup d'autres étudiants, de lire les sections du livre que vous prenez des cours supplémentaires. La plupart d'entre vous reviendront sur ce livre en tant que outil utile tout au long de vos futures études, notamment pour ceux d'entre vous qui poursuivent en informatique sciences, mathématiques et génie. J'ai conçu ce livre pour être une passerelle pour l'avenir études et explorations, et d'être une référence complète, et je vous souhaite bonne chance au début votre voyage.

Kenneth H. Rosen

CHAPITRE

Les fondations: Logique et preuves

Les règles de logique précisent la signification des énoncés mathématiques. Par exemple, ces règles aidez-nous à comprendre et à raisonner avec des énoncés tels que «Il existe un entier qui est pas la somme de deux carrés "et" Pour chaque entier positif n, la somme des entiers positifs ne dépassant pas n est $n(n + 1)/2$. »La logique est la base de tout raisonnement mathématique, et de tous raisonnement automatisé. Il a des applications pratiques à la conception de machines informatiques, à la spécification de systèmes, à l'intelligence artificielle, à la programmation informatique, à la programmation langues, et à d'autres domaines de l'informatique, ainsi qu'à de nombreux autres domaines d'études.

Pour comprendre les mathématiques, nous devons comprendre ce qui constitue une mathématique correcte argument, c'est-à-dire une preuve. Une fois que nous prouvons qu'un énoncé mathématique est vrai, nous l'appelons un théorème.UNE collection de théorèmes sur un sujet organiser ce que nous savons sur ce sujet. Apprendre un mathématique sujet, une personne doit construire activement des arguments mathématiques sur ce sujet, et pas seulement lire l'exposition. De plus, connaître la preuve d'un théorème permet souvent de modifier le résultat pour s'adapter à de nouvelles situations.

Tout le monde sait que les preuves sont importantes en mathématiques, mais beaucoup de gens trouvent il est surprenant de constater à quel point les preuves sont importantes en informatique.En fait, les preuves sont utilisées pour vérifier que les programmes informatiques produisent la sortie correcte pour toutes les valeurs d'entrée possibles, pour montrer que les algorithmes produisent toujours le résultat correct, pour établir la sécurité d'un système et pour créer intelligence artificielle. De plus, des systèmes de raisonnement automatisés ont été créés pour permettre ordinateurs pour construire leurs propres preuves.

Dans ce chapitre, nous expliquerons ce qui constitue un argument mathématique correct et créer des outils pour construire ces arguments. Nous développerons un arsenal de différentes méthodes de preuve cela nous permettra de prouver différents types de résultats. Après avoir introduit de nombreux méthodes de preuve, nous présenterons plusieurs stratégies de construction de preuves. Nous introduirons Donner la notion de conjecture et expliquer le processus de développement des mathématiques en étudiant conjectures.

Logique propositionnelle

introduction

Les règles de la logique donnent un sens précis aux énoncés mathématiques.Ces règles sont utilisées pour faire la distinction entre les arguments mathématiques valides et non valides. Parce qu'un objectif majeur de ce livre est d'apprendre au lecteur à comprendre et à construire des arguments mathématiques corrects, nous commençons notre étude des mathématiques discrètes par une introduction à la logique.

Outre l’importance de la logique dans la compréhension du raisonnement mathématique, la logique a nombreuses applications en informatique. Ces règles sont utilisées dans la conception des circuits informatiques, la construction de programmes informatiques, la vérification de l'exactitude des programmes et, en particulier, de nombreuses autres façons. En outre, des systèmes logiciels ont été développés pour construire certains, mais pas tous, types de preuves automatiquement.Nous allons discuter de ces applications de la logique dans ce domaine et chapitres ultérieurs.

Propositions

Notre discussion commence par une introduction aux éléments de base de la logique - les propositions. Une **proposition** est une phrase déclarative (c'est-à-dire une phrase qui déclare un fait) qui est soit vraie ou faux, mais pas les deux.

EXEMPLE 1 Toutes les phrases déclaratives suivantes sont des propositions.

1. Washington, DC, est la capitale des États-Unis d'Amérique.
2. Toronto est la capitale du Canada.
3. 1 + 1 = 2.
4. 2 + 2 = 3.

Les propositions 1 et 3 sont vraies, tandis que 2 et 4 sont fausses. ▲

Certaines phrases qui ne sont pas des propositions sont données dans l'exemple 2.

EXEMPLE 2 Considérez les phrases suivantes.

1. Quelle heure est-il?
2. Lisez ceci attentivement.
3. $x + 1 = 2$.
4. $x + y = z$.

Les phrases 1 et 2 ne sont pas des propositions car ce ne sont pas des phrases déclaratives.Peines 3 et 4 ne sont pas des propositions car elles ne sont ni vraies ni fausses.Notez que chacune des phrases 3 et 4 peut être transformé en proposition si nous attribuons des valeurs aux variables.Nous discuterons également d'autres façons de transformer des phrases comme celles-ci en propositions dans la section 1.4. ▲

Nous utilisons des lettres pour désigner des**variables propositionnelles** (ou **variables d'énoncé**), c'est-à-dire aptes qui représentent des propositions, tout comme les lettres sont utilisées pour désigner des variables numériques.le

Aristote (384 BCE-322 BCE) AristotlewasborninStagirus (Stagira) innorthernGreece.Hisfatherwas le médecin personnel du roi de Macédoine. Parce que son père est mort quand Aristote était jeune, Aristote ne pouvait pas suivre la coutume de suivre la profession de son père. Aristote est devenu orphelin à un jeune âge quand sa mère est également décédée. Son tuteur qui l'a élevé lui a enseigné la poésie, la rhétorique et le grec. À l'âge de Le 17, son tuteur l'envoya à Athènes pour poursuivre ses études. Aristote a rejoint l'Académie de Platon, où pendant 20 années, il a assisté aux conférences de Platon, présentant plus tard ses propres conférences sur la rhétorique. Quand Platon est mort en 347 avant notre ère , Aristote n'a pas été choisi pour lui succéder parce que ses vues différaient trop de celles de Platon. Au lieu, Aristote a rejoint la cour du roi Hermeas où il est resté pendant trois ans, et a épousé la nièce du Roi. Lorsque les Perses ont vaincu Hermeas, Aristote a déménagé à Mytilène et, à l'invitation du roi Philippe de Macédoine, il a enseigné à Alexandre, le fils de Philippe, qui est devenu plus tard Alexandre le Grand. Aristote a dirigé Alexander pendant cinq ans et après la mort du roi Philippe, il est retourné à Athènes et a créé sa propre école, appelée le lycée.

Les disciples d'Aristote étaient appelés les péripatéticiens, ce qui signifie «se promener», car Aristote se promenait souvent discuté des questions philosophiques. Aristote a enseigné au lycée pendant 13 ans où il a enseigné à ses étudiants avancés dans le matin et a donné des conférences populaires à un large public dans la soirée. Quand Alexandre le Grand est mort en 323 avant notre ère , une réaction violente contre tout ce qui concernait Alexandre menait à des accusations d'impiété contrefaites contre Aristote. Aristote s'est enfui à Chalcis pour éviter d'être poursuivi. Il n'a vécu qu'un an à Chalcis, mourant d'une maladie de l'estomac en 322 avant notre ère .

Aristote a écrit trois types d'œuvres: celles écrites pour un public populaire, des compilations de faits scientifiques et systématiques traités. Les traités systématiques comprenaient des travaux sur la logique, la philosophie, la psychologie, la physique et l'histoire naturelle. Écrits d'Aristote ont été conservés par un étudiant et ont été cachés dans un coffre-fort où un riche collectionneur de livres les a découverts environ 200 ans plus tard. Ils ont été emmenés à Rome, où ils ont été étudiés par des savants et publiés dans de nouvelles éditions, les conservant pour la postérité.

les lettres conventionnelles utilisées pour les variables propositionnelles sont $p, q, r, s, \ldots$. La **valeur** de **vérité** d'un proposition est vraie, notée T, si c'est une proposition vraie, et la valeur de vérité d'une proposition est faux, noté F, s'il s'agit d'une fausse proposition.

Le domaine de la logique qui traite des propositions est appelé le **calcul propositionnel** ou **propo- logique logique** . Il a d'abord été développé systématiquement par le philosophe grec Aristote plus il y a 2300 ans.

Nous nous tournons maintenant vers les méthodes de production de nouvelles propositions à partir de Nous avons déjà. Ces méthodes ont été discutées par le mathématicien anglais George Boole en 1854 dans son livre *Les lois de la pensée.* De nombreux énoncés mathématiques sont construits par combiner une ou plusieurs propositions. Les nouvelles propositions, appelées **propositions composées** , sont formé à partir de propositions existantes utilisant des opérateurs logiques.

DÉFINITION 1 Soit p une proposition. La *négation de p* , notée par p (également désignée par p), est la déclaration

"Ce n'est pas le cas que p ."

La proposition $\neg p$ se lit «non p ». La valeur de vérité de la négation de p , $\neg p$, est l'opposé de la valeur de vérité de p .

EXEMPLE 3 Trouver la négation de la proposition

«Le PC de Michael tourne sous Linux»

et l'exprimer en anglais simple.

Solution: la négation est

"Ce n'est pas le cas que le PC de Michael tourne sous Linux."

Cette négation peut être exprimée plus simplement comme

"Le PC de Michael ne fonctionne pas sous Linux."

▲

EXEMPLE 4 Trouver la négation de la proposition

"Le smartphone de Vandana a au moins 32 Go de mémoire"

et l'exprimer en anglais simple.

Solution: la négation est

"Ce n'est pas le cas que le smartphone de Vandana dispose d'au moins 32 Go de mémoire."

Cette négation peut également être exprimée comme

«Le smartphone de Vandana n'a pas au moins 32 Go de mémoire»

ou encore plus simplement

"Le smartphone de Vandana a moins de 32 Go de mémoire."

▲

TABLEAU 1 **Le Table de vérité pour la négation d'un Proposition.**

p	$\neg p$
T	F
F	T

Le tableau 1 affiche la **table de vérité** pour la négation d'une proposition p . Ce tableau a une ligne pour chacune des deux valeurs de vérité possibles d'une proposition p . Chaque ligne montre la valeur de vérité de $\neg p$ correspondant à la valeur de vérité de p pour cette ligne.

La négation d'une proposition peut également être considérée comme le résultat du fonctionnement du **opérateur de négation** sur une proposition. L'opérateur de négation construit une nouvelle proposition à partir de une seule proposition existante. Nous allons maintenant présenter les opérateurs logiques utilisés pour former de nouvelles propositions à partir de deux ou plusieurs propositions existantes.Ces opérateurs logiques sont également appelés **connecteurs** .

DÉFINITION 2 Soit p et q *des* propositions. La *conjonction* de p et q , notée $p \wedge q$, est la proposition « P et q ». La conjonction $p \wedge q$ est vraie lorsque p et q sont vraies et fausse sinon.

Le tableau 2 affiche la table de vérité de $p \wedge q$. Ce tableau comporte une ligne pour chacun des quatre possibles combinaisons de valeurs de vérité de p et q . Les quatre rangées correspondent aux paires de valeurs de vérité TT, TF, FT et FF, où la première valeur de vérité dans la paire est la valeur de vérité de p et la seconde la valeur de vérité est la valeur de vérité de q .

Notez qu'en logique, le mot «mais» est parfois utilisé à la place de «et» dans une conjonction.Pour exemple, la déclaration «Le soleil brille, mais il pleut» est une autre façon de dire «Le soleil brille et il pleut. »(Dans le langage naturel, il y a une subtile différence de sens entre «Et» et «mais»; nous ne nous préoccuperons pas de cette nuance ici.)

EXEMPLE 5 Trouver la conjonction des propositions p et q où p est la proposition «Le PC de Rebecca a plus de 16 Go d'espace libre sur le disque dur "et q est la proposition" Le processeur de Rebecca Le PC tourne plus vite que 1 GHz. ”

Solution: La conjonction de ces propositions, $p \wedge q$, est la proposition «Le PC de Rebecca a plus de 16 Go d'espace libre sur le disque dur, et le processeur du PC de Rebecca tourne plus vite que 1 GHz. "Cette conjonction peut être exprimée plus simplement comme" le PC de Rebecca a plus de 16 Go l'espace libre sur le disque dur, et son processeur tourne plus vite que 1 GHz. "Pour que cette conjonction soit vraie, les deux conditions données doivent être vraies.Elle est fausse lorsque l'une de ces conditions ou les deux sont fausses.▲

DÉFINITION 3 Soit p et q *des* propositions. La *disjonction* de p et q , notée $p \vee q$, est la proposition « P ou q ». La disjonction $p \vee q$ est fausse lorsque p et q sont toutes les deux fausses et vraie sinon.

Le tableau 3 affiche la table de vérité pour $p \vee q$.

TABLEAU 2 **La table de vérité pour la conjonction de deux Propositions.**

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

TABLEAU 3 **La table de vérité pour la disjonction de deux Propositions.**

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

L'utilisation du conjonctif *ou* en disjonction correspond à l'une des deux façons dont le mot *ou* est utilisé en anglais, à savoir en tant **qu'inclusif ou** . Une disjonction est vraie quand au moins l'un des deux propositions sont vraies. Par exemple, l'inclusif ou est utilisé dans l'instruction

"Les étudiants qui ont pris le calcul ou l'informatique peuvent suivre ce cours."

Ici, nous voulons dire que les étudiants qui ont suivi à la fois le calcul et l'informatique peuvent classe, ainsi que les étudiants qui n'ont suivi qu'une des deux matières.D'autre part, nous utilisons l' **exclusivité ou** quand nous disons

"Les étudiants qui ont suivi le calcul ou l'informatique, mais pas les deux, peuvent s'inscrire à ce classe."

Ici, nous voulons dire que les étudiants qui ont suivi des cours de calcul et d'informatique ne peuvent pas prenez le cours. Seuls ceux qui ont suivi exactement l'un des deux cours peuvent suivre le cours.

De même, quand un menu dans un restaurant dit: «La soupe ou la salade est accompagnée d'un plat principal», restaurant signifie presque toujours que les clients peuvent avoir de la soupe ou de la salade, mais pas les deux. Par conséquent, il s'agit d'une exclusivité plutôt que d'une inclusion ou.

EXEMPLE 6 Quelle est la disjonction des propositions p et q où p et q sont les mêmes propositions que dans l'exemple 5?

Solution: La disjonction de p et q , $p \vee q$, est la proposition

«Le PC de Rebecca dispose d'au moins 16 Go d'espace libre sur le disque dur, ou le processeur du PC de Rebecca tourne plus vite que 1 GHz. "

Cette proposition est vraie lorsque le PC de Rebecca dispose d'au moins 16 Go d'espace libre sur le disque dur, lorsque le Le processeur du PC fonctionne à une vitesse supérieure à 1 GHz et lorsque les deux conditions sont remplies.C'est faux quand les deux de ces conditions sont fausses, c'est-à-dire lorsque le PC de Rebecca a moins de 16 Go de disque dur libre l'espace et le processeur de son PC fonctionne à 1 GHz ou moins. ▲

Comme cela a été précédemment remarqué, l'utilisation du conjonctif *ou* en disjonction correspond à l'une des deux façons dont le mot *or* est utilisé en anglais, à savoir de manière inclusive. Ainsi, un la disjonction est vraie quand au moins une des deux propositions est vraie.Parfois, nous utilisons *ou* dans un sens exclusif. Lorsque l'exclusif ou est utilisé pour relier les propositions p et q , le la proposition « p ou q (mais pas les deux)» est obtenue.Cette proposition est vraie lorsque p est vrai et q est false, et lorsque p est faux et q est vrai. Il est faux lorsque p et q sont tous deux faux et lorsque les deux sont vrai.

GEORGE BOOLE (1815-1864) George Boole, le fils d'un cordonnier, est né à Lincoln, en Angleterre, en Novembre 1815. En raison de la situation financière difficile de sa famille, Boole a du mal à se soutenir sa famille. Néanmoins, il est devenu l'un des mathématiciens les plus importants des années 1800. Bien que il envisageait une carrière de membre du clergé, il décida plutôt d'aller dans l'enseignement et ouvrit peu après un son école. Dans sa préparation à l'enseignement des mathématiques, Boole - insatisfait des manuels de son époque - décida de lire les travaux des grands mathématiciens. En lisant les articles du grand mathématicien français Lagrange, Boole a fait des découvertes dans le calcul des variations, la branche d'analyse traitant de la découverte courbes et surfaces en optimisant certains paramètres.

En 1848, Boole publie *The Mathematical Analysis of Logic* , la première de ses contributions à la logique symbolique. En 1849, il est nommé professeur de mathématiques au Queen's College de Cork, en Irlande. En 1854, il publie *The Laws of Thought* , son œuvre la plus célèbre. Dans ce livre, Boole a présenté ce qu'on appelle maintenant *l'algèbre de Boole* en son honneur. Boole a écrit des manuels sur les équations différentielles et sur les équations aux différences utilisées en Grande-Bretagne jusqu'à la fin du XIXe siècle. Boole marié en 1855; sa femme était la nièce du professeur de grec au Queen's College. En 1864, Boole est décédé d'une pneumonie, il s'est contracté à la suite d'un engagement de conférence même s'il était trempé par une tempête de pluie.

TABLEAU 4 La table de vérité pour l'exclusif ou deux Propositions.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

TABLEAU 5 La table de vérité pour la déclaration conditionnelle $p \to q$.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

DÉFINITION 4 Soit p et q *des* propositions. L' *exclusif ou* de p et q , noté $p \oplus q$, est la proposition cela est vrai quand exactement l'un de p et q est vrai et faux sinon.

La table de vérité pour l'exclusivité ou pour deux propositions est affichée dans le tableau 4.

Expressions conditionnelles

Nous discuterons de plusieurs autres façons importantes de combiner des propositions.

DÉFINITION 5 Soit p et q *des* propositions. L' *énoncé conditionnel* $p \to q$ est la proposition «si p , alors q . »L'instruction conditionnelle $p \to q$ est fausse lorsque p est vraie et q est fausse, et vraie sinon. Dans l'énoncé conditionnel $p \to q$, p est appelé l' *hypothèse* (ou *antécédent* ou *prémisse*) et q est appelé la *conclusion* (ou la *conséquence*).

L'instruction $p \to q$ est appelée une instruction conditionnelle car $p \to q$ affirme que q est vrai à condition que p tienne. Une instruction conditionnelle est également appelée **implication** .

La table de vérité pour l'instruction conditionnelle $p \to q$ est présentée dans le tableau 5. Notez que l'énoncé $p \to q$ est vrai lorsque p et q sont vrais et quand p est faux (quelle que soit la vérité valeur q a).

Étant donné que les énoncés conditionnels jouent un rôle si essentiel dans le raisonnement mathématique, un une variété de terminologie est utilisée pour exprimer $p \to q$. Vous rencontrerez la plupart sinon la totalité des façons d'exprimer cette déclaration conditionnelle:

"Si p , alors q "	" P implique q "
"Si p , q "	" P seulement si q "
" P est suffisant pour q "	"Une condition suffisante pour q est p "
" Q si p "	" Q chaque fois que p "
" Q quand p "	" Q est nécessaire pour p "
"Une condition nécessaire pour p est q "	" Q découle de p "
" Q *à* moins que $\neg p$ "	

Un moyen utile de comprendre la valeur de vérité d'une déclaration conditionnelle est de penser à un obligation ou un contrat. Par exemple, l'engagement de nombreux politiciens lorsqu'ils se présentent aux élections est

«Si je suis élu, je réduirai les impôts.»

Si le politicien est élu, les électeurs s'attendraient à ce qu'il baisse les impôts.De plus, si le le politicien n'est pas élu, les électeurs n'auront aucune attente que cette personne baisse les impôts, bien que la personne puisse avoir une influence suffisante pour faire baisser les impôts des personnes au pouvoir. Ce n'est que lorsque le politicien est élu mais n'abaisse pas les impôts que les électeurs peuvent dire que le politicien a rompu l'engagement de campagne. Ce dernier scénario correspond au cas où p est vrai mais q est faux dans $p \to q$.

De même, considérons une déclaration qu'un professeur pourrait faire:

"Si vous obtenez 100% sur la finale, vous obtiendrez un A."

Si vous parvenez à obtenir un 100% sur la finale, alors vous vous attendez à recevoir un A. Si vous ne le faites pas obtenir 100%, vous pouvez ou non recevoir un A en fonction d'autres facteurs. Cependant, si vous obtenez 100%, mais le professeur ne vous donne pas de A, vous vous sentirez trompé.

Parmi les différentes façons d'exprimer l'énoncé conditionnel $p \to q$, les deux qui semblent causer les plus confus sont « p seulement si q » et « q sauf si $\neg p$ ». Par conséquent, nous fournirons quelques des conseils pour dissiper cette confusion.

Pour se rappeler que « p seulement si q » exprime la même chose que «si p , alors q », notez que « p seulement si q "dit que p ne peut pas être vrai quand q n'est pas vrai. Autrement dit, la déclaration est fausse si p est vrai, mais q est faux. Lorsque p est faux, q peut être vrai ou faux, car l'instruction ne dit rien sur la valeur de vérité de q . Attention à ne pas utiliser « q uniquement si p » pour exprimer $p \to q$ car c'est Incorrect. Pour voir cela, notez que les vraies valeurs de « q seulement si p » et $p \to q$ sont différentes lorsque p et q ont des valeurs de vérité différentes.

Vous pourriez avoir du mal comprendre comment «Sauf» est utilisé dans expressions conditionnelles sauf si vous lisez ceci soigneusement.

Pour se rappeler que « q *à* moins que $\neg p$ » exprime la même déclaration conditionnelle que «si p , alors q », notez que« q *à* moins que $\neg p$ »signifie que si $\neg p$ est faux, alors q doit être vrai. Autrement dit, la déclaration " Q *à* moins que $\neg p$ " soit faux quand p est vrai mais q est faux, mais c'est vrai autrement. Par conséquent, « Q *à* moins que $\neg p$ » et $p \to q$ aient toujours la même valeur de vérité.

Nous illustrons la traduction entre les déclarations conditionnelles et les déclarations en anglais dans Example 7.

EXEMPLE 7 Soit p l'énoncé «Maria apprend les mathématiques discrètes» et q l'énoncé «Maria va trouver un bon emploi. »Exprimez la déclaration $p \to q$ sous forme de déclaration en anglais.

Solution: à partir de la définition des instructions conditionnelles, nous voyons que lorsque p est l'instruction «Maria apprend les mathématiques discrètes» et q est l'énoncé «Maria trouvera un bon emploi», $p \to q$ représente la déclaration

"Si Maria apprend des mathématiques discrètes, alors elle trouvera un bon travail."

Il existe de nombreuses autres façons d'exprimer cette déclaration conditionnelle en anglais.Parmi les plus naturels de ceux-ci sont:

«Maria trouvera un bon emploi lorsqu'elle apprend des mathématiques discrètes.»

«Pour que Maria obtienne un bon emploi, il lui suffit d'apprendre des mathématiques discrètes.»

et

«Maria trouvera un bon emploi à moins qu'elle n'apprenne des mathématiques discrètes.» ▲

Notez que la façon dont nous avons défini les instructions conditionnelles est plus générale que la signification attaché à ces déclarations en langue anglaise. Par exemple, l'instruction conditionnelle dans Exemple 7 et l'instruction

"S'il fait beau, nous irons à la plage."

sont des déclarations utilisées dans un langage normal où il existe une relation entre l'hypothèse et la conclusion. De plus, la première de ces déclarations est vraie à moins que Maria apprenne discrète mathématiques, mais elle ne fait pas un bon travail, et la seconde est vraie à moins qu'il ne soit en effet ensoleillé, mais on ne va pas à la plage.D'un autre côté, la déclaration

"Si Juan a un smartphone, alors 2 + 3 = 5"

est vrai à partir de la définition d'une instruction conditionnelle, car sa conclusion est vraie.(La vérité la valeur de l'hypothèse n'a alors plus d'importance.) L'instruction conditionnelle

"Si Juan a un smartphone, alors 2 + 3 = 6"

est vrai si Juan n'a pas de smartphone, même si 2 + 3 = 6 est faux.Nous n'utiliserions pas ces deux dernières déclarations conditionnelles en langage naturel (sauf peut-être dans le sarcasme), parce que il n'y a pas de relation entre l'hypothèse et la conclusion dans l'une ou l'autre affirmation.En mathématiques le raisonnement ématique, nous considérons les déclarations conditionnelles d'un type plus général que nous utilisons dans Anglais. Le concept mathématique d'un énoncé conditionnel est indépendant d'une cause et relation d'effet entre l'hypothèse et la conclusion. Notre définition d'une déclaration conditionnelle précise ses valeurs de vérité; il n'est pas basé sur l'utilisation de l'anglais.Le langage propositionnel est un artificiel Langue; nous utilisons uniquement l'anglais en parallèle pour le rendre facile à utiliser et à mémoriser.

La construction if-then utilisée dans de nombreux langages de programmation est différente de celle utilisée en logique. La plupart des langages de programmation contiennent des instructions telles que**si** p **puis** S , où p est un proposition et S est un segment de programme (une ou plusieurs instructions à exécuter).Quand exécution d'un programme rencontre une telle instruction, S est exécuté si p est vrai, mais S n'est pas exécuté si p est faux, comme illustré dans l'exemple 8.

EXEMPLE 8 Quelle est la valeur de la variable x après l'instruction

si $2 + 2 = 4$ **alors** $x := x + 1$

si $x = 0$ avant que cette instruction ne soit rencontrée? (Le symbole: = signifie affectation. Le instruction $x := x + 1$ signifie l'affectation de la valeur de $x + 1$ à x .)

Solution: comme $2 + 2 = 4$ est vrai, l'instruction d'affectation $x := x + 1$ est exécutée. Par conséquent, x a la valeur $0 + 1 = 1$ une fois cette instruction rencontrée. ▲

CONVERSE, CONTRAPOSITIVE ET INVERSE Nous pouvons former de nouvelles conditions instructions commençant par une instruction conditionnelle $p \to q$. En particulier, il existe trois les instructions conditionnelles qui se produisent si souvent qu'elles ont des noms spéciaux.La proposition $q \to p$ est appelé l' **inverse** de $p \to q$. La **contrapositive** de $p \to q$ est la proposition $\neg q \to \neg p$. La proposition $\neg p \to \neg q$ est appelée l' **inverse** de $p \to q$. Nous verrons que de ces trois déclarations conditionnelles formées de $p \to q$, seul le contrapositif a toujours la même vérité valeur comme $p \to q$.

Nous montrons d'abord que la contrapositive, $\neg q \to \neg p$, d'un énoncé conditionnel $p \to q$ toujours a la même valeur de vérité que $p \to q$. Pour voir cela, notez que la contrapositive n'est fausse que lorsque $\neg p$ est faux et $\neg q$ est vrai, c'est-à-dire uniquement lorsque p est vrai et q est faux. Nous montrons maintenant que ni l'inverse, $q \to p$, ni l'inverse, $\neg p \to \neg q$, a la même valeur de vérité que $p \to q$ pour tous valeurs de vérité possibles de p et q . Notez que lorsque p est vrai et q est faux, le conditionnel d'origine est fausse, mais l'inverse et l'inverse sont tous deux vrais.

N'oubliez pas que le contrapositif, mais ni

Lorsque deux propositions composées ont toujours la même valeur de vérité, nous les appelons **équivalentes.**

l'inverse ou l'inverse, de une déclaration conditionnelle est équivalent à elle.

alentour , de sorte qu'une instruction conditionnelle et sa contrapositive sont équivalentes.L'inverse et l'inverse d'une instruction conditionnelle sont également équivalents, comme le lecteur peut le vérifier, mais équivalent à l'énoncé conditionnel d'origine. (Nous étudierons des propositions équivalentes dans 1.3.) Notez que l'une des erreurs logiques les plus courantes est de supposer que l'inverse ou l'inverse d'une instruction conditionnelle est équivalent à cette instruction conditionnelle.

Nous illustrons l'utilisation des instructions conditionnelles dans l'exemple 9.

EXEMPLE 9 Quels sont le contrapositif, l'inverse et l'inverse de l'énoncé conditionnel

"L'équipe à domicile gagne chaque fois qu'il pleut?"

Solution: parce que « q chaque fois que p » est l'un des moyens d'exprimer l'instruction conditionnelle $p \to q$, la déclaration d'origine peut être réécrite comme

"S'il pleut, l'équipe à domicile gagne."

Par conséquent, le contrapositif de cette déclaration conditionnelle est

"Si l'équipe à domicile ne gagne pas, il ne pleut pas."

L'inverse est

"Si l'équipe à domicile gagne, alors il pleut."

L'inverse est

"S'il ne pleut pas, l'équipe à domicile ne gagne pas."

Seul le contrapositif est équivalent à la déclaration d'origine. ▲

BICONDITIONNELS Nous introduisons maintenant une autre façon de combiner des propositions qui expriment que deux propositions ont la même valeur de vérité.

DÉFINITION 6 Soit p et q *des* propositions. L' *énoncé biconditionnel* $p \leftrightarrow q$ est la proposition « p si et seulement si q . »L'énoncé biconditionnel $p \leftrightarrow q$ est vrai quand p et q ont la même vérité valeurs, et est faux sinon.Les déclarations biconditionnelles sont également appelées *bi-implications* .

La table de vérité pour $p \leftrightarrow q$ est présentée dans le tableau 6. Notez que l'énoncé $p \leftrightarrow q$ est vrai lorsque les deux les énoncés conditionnels $p \to q$ et $q \to p$ sont vrais et faux sinon.C'est pourquoi nous utilisons les mots «si et seulement si» pour exprimer ce connecteur logique et pourquoi il est écrit symboliquement en combinant les symboles → et ←.Il existe d'autres façons courantes d'exprimer $p \leftrightarrow q$:

" P est nécessaire et suffisant pour q "
"Si p alors q , et inversement"
" P q si q ."

La dernière façon d'exprimer l'énoncé biconditionnel $p \leftrightarrow q$ utilise l'abréviation «iff» pour «Si et seulement si». Notez que $p \leftrightarrow q$ a exactement la même valeur de vérité que $(p \to q) \wedge (q \to p)$.

TABLEAU 6 **La table de vérité pour Biconditional $p \leftrightarrow q$.**

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

EXEMPLE 10 Soit p la déclaration «vous pouvez prendre le vol» et q soit la déclaration «vous achetez un billet». Alors $p \leftrightarrow q$ est la déclaration

"Vous pouvez prendre le vol si et seulement si vous achetez un billet."

Cette affirmation est vraie si p et q sont tous deux vrais ou tous deux faux, c'est-à-dire si vous achetez un billet et peut prendre le vol ou si vous n'achetez pas de billet et que vous ne pouvez pas prendre le vol. C'est faux quand p et q ont des valeurs de vérité opposées, c'est-à-dire lorsque vous n'achetez pas de ticket, mais que vol (par exemple lorsque vous obtenez un voyage gratuit) et lorsque vous achetez un billet mais que vous ne pouvez pas prendre le vol (comme lorsque la compagnie aérienne vous heurte). ▲

UTILISATION IMPLICITE DES BICONDITIONNELS Vous devez savoir que les biconditionnels ne sont pas toujours explicite en langage naturel. En particulier, la construction «si et seulement si» utilisée dans biconditionals est rarement utilisé dans le langage courant. Au lieu de cela, les conditions biconditionnelles sont souvent exprimées en utilisant une construction «si, alors» ou «seulement si». L'autre partie du «si et seulement si» est implicite. Autrement dit, l'inverse est implicite, mais non déclaré. Par exemple, considérez la déclaration en anglais "Si vous terminez votre repas, vous pouvez prendre un dessert." Ce que cela signifie vraiment, c'est "Vous pouvez avoir dessert si et seulement si vous avez terminé votre repas. "Cette dernière déclaration est logiquement équivalente à la deux déclarations «Si vous terminez votre repas, vous pouvez prendre un dessert» et «Vous pouvez prendre un dessert que si vous avez terminé votre repas. "En raison de cette imprécision du langage naturel, nous devons faire l'hypothèse si une déclaration conditionnelle en langage naturel inclut implicitement son converser. Parce que la précision est essentielle en mathématiques et en logique, nous distinguerons toujours entre l'instruction conditionnelle $p \rightarrow q$ et l'instruction biconditionnelle $p \leftrightarrow q$.

Tables de vérité des propositions composées

Nous avons maintenant introduit quatre connecteurs logiques importants: conjonctions, disjonctions, con- les déclarations conditionnelles et les déclarations biconditionnelles, ainsi que les négations. Nous pouvons utiliser ces con- nectifs pour construire des propositions composées complexes impliquant un certain nombre de propositions variables. Nous pouvons utiliser des tables de vérité pour déterminer les valeurs de vérité de ces propositions composées, comme l'illustre l'exemple 11. Nous utilisons une colonne distincte pour trouver la valeur de vérité de chaque composé expression qui se produit dans la proposition composée au fur et à mesure qu'elle se construit. Les valeurs de vérité du proposition composée pour chaque combinaison de valeurs de vérité des variables propositionnelles se trouve dans la dernière colonne du tableau.

EXEMPLE 11 Construire la table de vérité de la proposition composée

$$(p \vee \neg q) \rightarrow (p \wedge q).$$

Solution: Parce que cette table de vérité implique deux variables propositionnelles p et q , il y a quatre lignes dans cette table de vérité, une pour chacune des paires de valeurs de vérité TT, TF, FT et FF. La première deux colonnes sont utilisées pour les valeurs de vérité de p et q , respectivement. Dans la troisième colonne, nous trouvons la valeur de vérité de $\neg q$, nécessaire pour trouver la valeur de vérité de $p \vee \neg q$, trouvée dans la quatrième colonne. le la cinquième colonne donne la valeur de vérité de $p \wedge q$. Enfin, la valeur de vérité de $(p \vee \neg q) \rightarrow (p \wedge q)$ est trouvé dans la dernière colonne. La table de vérité résultante est présentée dans le tableau 7. ▲

TABLEAU 7 **La table de vérité de $(p \vee \neg q) \rightarrow (p \wedge q)$.**

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \rightarrow (p \wedge q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	F	T
F	F	T	T	F	F

Priorité des opérateurs logiques

Nous pouvons construire des propositions composées en utilisant l'opérateur de négation et les opérateurs logiques défini jusqu'à présent. Nous utiliserons généralement des parenthèses pour spécifier l'ordre dans lequel les opérateurs logiques dans une proposition composée doivent être appliqués. Par exemple, $(p \vee q) \wedge (\neg r)$ est la conjonction de $p \vee q$ et $\neg r$. Cependant, pour réduire le nombre de parenthèses, nous précisons que la négation L'opérateur est appliqué avant tous les autres opérateurs logiques. Cela signifie que $\neg p \wedge q$ est la conjonction of $\neg p$ et q , à savoir $(\neg p) \wedge q$, et non la négation de la conjonction de p et q , à savoir $\neg (p \wedge q)$.

Une autre règle générale de priorité est que l'opérateur de conjonction a priorité sur l'opérateur de disjonction, de sorte que $p \wedge q \vee r$ signifie $(p \wedge q) \vee r$ plutôt que $p \wedge (q \vee r)$. Car cette règle peut être difficile à retenir, nous continuerons à utiliser des parenthèses afin que l'ordre des les opérateurs de disjonction et de conjonction sont clairs.

Enfin, c'est une règle acceptée que les opérateurs conditionnels et biconditionnels $\rightarrow$ et $\leftrightarrow$ ont une priorité plus faible que les opérateurs de conjonction et de disjonction, $\wedge$ et $\vee$. Par conséquent, $p \vee q \rightarrow r$ est identique à $(p \vee q) \rightarrow r$. Nous utiliserons des parenthèses lorsque l'ordre de la

L'opérateur conditionnel et l'opérateur biconditionnel sont en cause, bien que l'opérateur conditionnel ait priorité sur l'opérateur biconditionnel. Le tableau 8 affiche les niveaux de priorité de la logique opérateurs, $\neg$, $\wedge$, $\vee$, $\rightarrow$ et $\leftrightarrow$.

TABLEAU 8
Priorité de Opérateurs logiques.

Opérateur	*Priorité*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Opérations de logique et de bits

Les ordinateurs représentent des informations à l'aide de bits. Un **bit** est un symbole avec deux valeurs possibles, à savoir, 0 (zéro) et 1 (un). Cette signification du bit de mot vient de *b* inaire creuser *ce* , parce que des zéros et les uns sont les chiffres utilisés dans les représentations binaires des nombres. Le statisticien bien connu John Tukey a introduit cette terminologie en 1946. Un peu peut être utilisé pour représenter une valeur de vérité, car il y a deux valeurs de vérité, à savoir *vrai* et *faux* . Comme d'habitude, nous utiliserons un bit pour représente vrai et un bit 0 pour représenter faux. Autrement dit, 1 représente T (vrai), 0 représente F (faux). UNE La variable est appelée **variable booléenne** si sa valeur est vraie ou fausse. Par conséquent, un booléen variable peut être représentée à l'aide d'un bit.

Valeur de vérité	*Bit*
T	1
F	0

Les **opérations sur les bits** informatiques correspondent aux connecteurs logiques. En remplaçant true par un et faux par un zéro dans les tables de vérité pour les opérateurs $\wedge$, $\vee$ et $\oplus$, les tables présentées dans le tableau 9 pour les opérations binaires correspondantes sont obtenues. Nous utiliserons également la notation *OR* , *AND* et *XOR* pour les opérateurs $\vee$, $\wedge$ et $\oplus$, comme cela se fait dans différents langages de programmation.

JOHN WILDER TUKEY (1915–2000) Tukey, né à New Bedford, Massachusetts, était enfant unique. Le sien les parents, les deux enseignants, ont décidé que l'enseignement à domicile développerait le mieux son potentiel. Son éducation formelle a commencé à l'Université Brown, où il a étudié les mathématiques et la chimie. Il a obtenu une maîtrise en chimie de Brown et a poursuivi ses études à l'Université de Princeton, changeant son domaine d'études de la chimie à mathématiques. Il a obtenu son doctorat. de Princeton en 1939 pour un travail en topologie, quand il a été nommé professeur de mathématiques à Princeton. Au début de la Seconde Guerre mondiale, il rejoint le Fire Control Research Office, où il a commencé à travailler dans les statistiques. Tukey a trouvé la recherche statistique à son goût et a impressionné plusieurs leaders statisticiens avec ses compétences. En 1945, à la fin de la guerre, Tukey retourne au département de mathématiques à Princeton en tant que professeur de statistique, et il a également pris un poste chez AT&T Bell Laboratories. Fondation de Tukey le Département de statistique à Princeton en 1966 et a été son premier président. Tukey a apporté des contributions importantes à de nombreux domaines statistiques, y compris l'analyse de la variance, l'estimation des spectres de séries chronologiques, les inférences sur les valeurs d'un ensemble de paramètres à partir d'une seule expérience, et la philosophie des statistiques. Cependant, il est surtout connu pour son invention, avec JW Cooley, du rapide Transformée de Fourier. En plus de ses contributions aux statistiques, Tukey était reconnu comme un expert en mots; il est crédité d'avoir inventé les termes *bit* et *logiciel* .

Tukey a apporté sa perspicacité et son expertise en siégeant au comité consultatif scientifique du président. Il a présidé plusieurs d'importants comités traitant de l'environnement, de l'éducation, des produits chimiques et de la santé. Il a également fait partie de comités travaillant sur le désarmement nucléaire. Tukey a reçu de nombreux prix, dont la Médaille nationale des sciences.

NOTE HISTORIQUE Il y avait plusieurs autres mots suggérés pour un chiffre binaire, y compris *binit* et *bigit* , qui n'ont jamais été largement accepté. L'adoption du mot *bit* peut être due à sa signification en tant que mot anglais courant. Pour un compte rendu de la création de Tukey du mot *bit* , voir le numéro d'avril 1984 des *Annales de l'histoire de l'informatique.*

TABLEAU 9 **Tableau des opérateurs de bits *OU*, *ET*, et *XOR*.**

X	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Les informations sont souvent représentées à l'aide de chaînes de bits, qui sont des listes de zéros et de unsQuand cela est fait, les opérations sur les chaînes de bits peuvent être utilisées pour manipuler ces informations.

DÉFINITION 7 Une *chaîne de bits* est une séquence de zéro ou plusieurs bits.La *longueur* de cette chaîne est le nombre de bits dans la chaîne.

L'EXEMPLE 12 101010011 est une chaîne de bits de longueur neuf. ▲

Nous pouvons étendre les opérations binaires aux chaînes binaires.Nous définissons le **bit à bit *OU***, **bit à bit *ET***, et ***XOR au niveau* du bit** de deux chaînes de même longueur pour être les chaînes qui ont comme bits le*OU*, *ET* et *XOR* des bits correspondants dans les deux chaînes, respectivement.Nous utilisons les symboles $\vee$, $\wedge$ et $\oplus$ pour représenter respectivement les opérations *OR* au niveau du bit, *ET au niveau du* bit et *XOR au niveau du* bit. Nous illustrons les opérations au niveau du bit sur les chaînes de bits avec l'exemple 13.

EXEMPLE 13 Trouver l' *OR au niveau* du bit, le *AND au niveau du* bit et le *XOR au niveau* du bit des chaînes de bits 0110110110 et 1100011101. (Ici et tout au long de ce livre, les chaînes de bits seront divisées en blocs de quatre pour les rendre plus lisibles.)

Solution: le bit *OR*, le bit *AND* et le bit *XOR* de ces chaînes sont obtenus en prenant les *OR*, *AND* et *XOR* des bits correspondants, respectivement. Cela nous donne

01 1011 0110
11 0001 1101

11 1011 1111 au niveau du bit *OU*
01 0001 0100 au niveau du bit *ET*
10 1010 1011 *XOR au niveau du* bit ▲

Des exercices

1. Laquelle de ces phrases sont des propositions? Quels sont les valeurs de vérité de ceux qui sont des propositions?
- **a)** Boston est la capitale du Massachusetts.
- **b)** Miami est la capitale de la Floride.
- **c)** 2 + 3 = 5.
- **d)** 5 + 7 = 10.
- **e)** $x + 2 = 11$.
- **f)** Répondez à cette question.

2. Quelles sont ces propositions? Quelles sont les valeurs de vérité de celles qui sont des propositions?
- **a)** Ne passez pas go.
- **b)** Quelle heure est-il?
- **c)** Il n'y a pas de mouches noires dans le Maine.
- **d)** $4 + x = 5$.
- **e)** La lune est faite de fromage vert.
- **f)** $2^n \geq 100$.

3. Quelle est la négation de chacune de ces propositions?
- **a)** Mei a un lecteur MP3.
- **b)** Il n'y a pas de pollution dans le New Jersey.
- **c)** 2 + 1 = 3.
- **d)** L'été dans le Maine est chaud et ensoleillé.

4. Quelle est la négation de chacune de ces propositions?
- **a)** Jennifer et Teja sont amis.
- **b)** Il y a 13 articles dans une douzaine de boulangers.
- **c)** Abby a envoyé plus de 100 messages texte chaque jour.
- **d)** 121 est un carré parfait.

5. Quelle est la négation de chacune de ces propositions?
- **a)** Steve a plus de 100 Go d'espace disque libre sur son portable.

10. Soit p et q les propositions «L'élection est décidée» et «Les votes ont été comptés», respectivement. Express chacune de ces propositions composées en tant que sen-

b) Zach bloque les courriels et les textes de Jennifer.
c) $7 \cdot 11 \cdot 13 = 999$.
d) Diane a roulé son vélo sur 100 milles dimanche.

6. Supposons que le smartphone A possède 256 Mo de RAM et 32 Go ROM, et la résolution de son appareil photo est de 8 MP; Intelligent-téléphone B a 288 Mo de RAM et 64 Go de ROM, et le la résolution de son appareil photo est de 4 MP; et le smartphone C a 128 Mo de RAM et 32 Go de ROM, et la résolution de son appareil photo est de 5 MP. Déterminer la valeur de vérité de chacun ces propositions.

a) Le smartphone B a le plus de RAM de ces trois smartphones. Téléphone (s.
b) Le smartphone C a plus de ROM ou une résolution supérieure appareil photo que Smartphone B.
c) Le smartphone B a plus de RAM, plus de ROM et un caméra de résolution supérieure à celle du Smartphone A.
d) Si le smartphone B a plus de RAM et plus de ROM que Smartphone C, alors il a également une résolution plus élevée caméra.
e) Le smartphone A a plus de RAM que le smartphone B si et seulement si le Smartphone B a plus de RAM que le Smart-téléphone A.

7. Supposons qu'au cours de la dernière année fiscale, Le chiffre d'affaires annuel d'Acme Computer s'élève à 138 milliards de dollars et son bénéfice net était de 8 milliards de dollars, le revenu annuel de Nadir Software était de 87 milliards de dollars et son bénéfice net était de 5 milliards de dollars, et le revenu annuel de Quichotte Les médias représentaient 111 milliards de dollars et son bénéfice net 13 milliards de dollars. Déterminer la valeur de vérité de chacun ces propositions pour le dernier exercice.

a) Quixote Media a enregistré les revenus annuels les plus importants.
b) Nadir Software avait le bénéfice net le plus bas et Acme L'ordinateur avait le plus gros revenu annuel.
c) Acme Computer avait le plus grand bénéfice net ou Quixote Les médias ont enregistré le bénéfice net le plus important.
d) Si Quixote Media avait le plus petit bénéfice net, alors Acme Computer a réalisé le plus gros chiffre d'affaires annuel.
e) Nadir Software avait le plus petit bénéfice net si et seulement si Acme Computer avait le plus gros revenu annuel.

8. Soit p et q les propositions

p : J'ai acheté un billet de loterie cette semaine.
q : J'ai gagné le jackpot d'un million de dollars.

Exprimez chacune de ces propositions en anglais tence.

a) $\neg p$ **b)** $p \vee q$ **c)** $p \rightarrow q$
d) $p \wedge q$ **e)** $p \leftrightarrow q$ **f)** $\neg p \rightarrow \neg q$
g) $\neg p \wedge \neg q$ **h)** $\neg p \vee (p \wedge q)$

9. Soit p et q les propositions «Nager au Nouveau La côte de Jersey est autorisée »et« Des requins ont été repérés près du rivage », respectivement. Exprimez chacune de ces com-propositions de livre comme une phrase anglaise.

a) $\neg q$ **b)** $p \wedge q$ **c)** $\neg p \vee q$
d) $p \rightarrow \neg q$ **e)** $\neg q \rightarrow p$ **f)** $\neg p \rightarrow \neg q$
g) $p \leftrightarrow \neg q$ **h)** $\neg p \wedge (p \vee \neg q)$

tence.

a) $\neg p$ **b)** $p \vee q$
c) $\neg p \wedge q$ **d)** $q \rightarrow p$
e) $\neg q \rightarrow \neg p$ **f)** $\neg p \rightarrow \neg q$
g) $p \leftrightarrow q$ **h)** $\neg q \vee (\neg p \wedge q)$

11. Soit p et q les propositions

p : Il est en dessous de zéro.
q : Il neige.

Écrivez ces propositions en utilisant p et q et la logique nectifs (y compris les négations).

a) Il est en dessous de zéro et de neige.
b) Il fait en dessous de zéro mais ne neige pas.
c) Il ne fait pas en dessous de zéro et il ne neige pas.
d) Il neige soit en dessous de zéro (ou les deux).
e) S'il fait en dessous de zéro, il neige également.
f) Soit il fait froid, soit il neige, mais il est ne neige pas s'il fait en dessous de zéro.
g) Qu'il soit inférieur au point de congélation est nécessaire et suffisant pour qu'il neige.

12. Soit p , q et r les propositions

p : Vous avez la grippe.
q : Vous manquez l'examen final.
r : Vous réussissez le cours.

Exprimez chacune de ces propositions en anglais tence.

a) $p \rightarrow q$ **b)** $\neg q \leftrightarrow r$
c) $q \rightarrow \neg r$ **d)** $p \vee q \vee r$
e) $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$
f) $(p \wedge q) \vee (\neg q \wedge r)$

13. Soit p et q les propositions

p : Vous conduisez plus de 65 miles par heure.
q : Vous obtenez un ticket pour excès de vitesse.

Écrivez ces propositions en utilisant p et q et la logique nectifs (y compris les négations).

a) Vous ne conduisez pas plus de 65 miles par heure.
b) Vous conduisez plus de 65 miles par heure, mais vous n'obtenez pas un excès de vitesse.
c) Vous obtiendrez un ticket pour excès de vitesse si vous conduisez 65 miles par heure.
d) Si vous ne conduisez pas plus de 65 miles par heure, vous ne recevra pas de contravention pour excès de vitesse.
e) Conduire plus de 65 miles par heure est suffisant pour obtenir un excès de vitesse.
f) Vous obtenez un ticket pour excès de vitesse, mais vous ne roulez pas 65 miles par heure.
g) Chaque fois que vous obtenez un ticket pour excès de vitesse, vous conduisez plus de 65 miles par heure.

14. Soit p , q et r les propositions

p : Vous obtenez un A à l'examen final.
q : Vous faites tous les exercices de ce livre.
r : Vous obtenez un A dans cette classe.

Écrivez ces propositions en utilisant p , q et r et logique connecteurs (y compris les négations).

a) Vous obtenez un A dans cette classe, mais vous ne faites pas tous les exercice dans ce livre.
b) Vous obtenez un A sur la finale, vous faites tous les exercices de cette livre, et vous obtenez un A dans cette classe.
c) Pour obtenir un A dans cette classe, il vous faut obtenir un A en finale.
d) Vous obtenez un A en finale, mais vous ne faites pas tous les exercice dans ce livre; néanmoins, vous obtenez un A dans ce classe.
e) Obtenir un A sur la finale et faire chaque exercice ce livre est suffisant pour obtenir un A dans cette classe.
f) Vous obtiendrez un A dans cette classe si et seulement si vous faites tous les exercices de ce livre ou vous obtenez un A sur le final.

15. Soit p , q et r les propositions

p : Des grizzlis ont été vus dans la région.
q : La randonnée est sécuritaire sur le sentier.
r : Les baies sont mûres le long du sentier.

Écrivez ces propositions en utilisant p , q et r et logique

a) Le café ou le thé vient avec le dîner.
b) Un mot de passe doit avoir au moins trois chiffres ou être à au moins huit caractères.
c) La condition préalable au cours est un cours en nombre théorie ou un cours de cryptographie.
d) Vous pouvez payer en dollars américains ou en euros.

20. Pour chacune de ces phrases, déterminez si un clusif ou, ou un exclusif ou, est destiné. Expliquez votre répondre.

a) Une expérience avec C ++ ou Java est requise.
b) Le déjeuner comprend une soupe ou une salade.
c) Pour entrer dans le pays, vous avez besoin d'un passeport ou d'un électeur carte d'enregistrement.
d) Publier ou périr.

21. Pour chacune de ces phrases, indiquez ce que signifie la phrase si le connecteur logique ou est un inclusif ou (c'est-à-dire un dis-jonction) par rapport à un ou exclusif. Laquelle de ces significations ou pensez-vous qu'il est destiné?

connecteurs (y compris les négations).

a) Les baies sont mûres le long du sentier, mais les grizzlis ont n'a pas été vu dans la région.

b) Les grizzlis n'ont pas été vus dans la région et sur le sentier est sûr, mais les baies sont mûres le long du Piste.

c) Si les baies sont mûres le long du sentier, la randonnée est sûre si et seulement si les grizzlis n'ont pas été vus dans la région.

d) Il n'est pas sûr de marcher sur le sentier, mais les grizzlis ont pas vu dans la région et les baies le long du sentier sont mûrs.

e) Pour que la randonnée sur le sentier soit sûre, il est nécessaire mais pas suffisant que les baies ne soient pas mûres le long du sentier et pour que les grizzlis n'aient pas été vus dans la région.

f) La randonnée n'est pas sécuritaire sur le sentier chaque fois que les grizzlis ont été vus dans la région et les baies sont mûres le sentier.

16. Déterminez si ces conditions biconditionnelles sont vraies ou faux.

a) $2 + 2 = 4$ si et seulement si $1 + 1 = 2$.

b) $1 + 1 = 2$ si et seulement si $2 + 3 = 4$.

c) $1 + 1 = 3$ si et seulement si les singes peuvent voler.

d) $0 > 1$ si et seulement si $2 > 1$.

17. Déterminez si chacune de ces déclarations conditionnelles est vrai ou faux.

a) Si $1 + 1 = 2$, alors $2 + 2 = 5$.

b) Si $1 + 1 = 3$, alors $2 + 2 = 4$.

c) Si $1 + 1 = 3$, alors $2 + 2 = 5$.

d) Si les singes peuvent voler, alors $1 + 1 = 3$.

18. Déterminez si chacune de ces déclarations conditionnelles est vrai ou faux.

a) Si $1 + 1 = 3$, alors les licornes existent.

b) Si $1 + 1 = 3$, les chiens peuvent voler.

c) Si $1 + 1 = 2$, les chiens peuvent voler.

d) Si $2 + 2 = 4$, alors $1 + 2 = 3$.

19. Pour chacune de ces phrases, déterminez si un clusif ou, ou un exclusif ou, est destiné. Expliquez votre répondre.

a) Pour prendre des mathématiques discrètes, vous devez avoir pris calcul ou un cours d'informatique.

b) Lorsque vous achetez une nouvelle voiture chez Acme Motor Company, vous obtenez 2000 $ en espèces ou un prêt auto de 2%.

c) Le dîner pour deux comprend deux articles de la colonne A ou trois éléments de la colonne B.

d) L' école est fermée s'il tombe plus de 2 pieds de neige ou si le refroidissement éolien est inférieur à -100.

22. Écrivez chacune de ces déclarations sous la forme «si p , alors q » en anglais. [*Astuce:* reportez - vous à la liste des moyens courants presse les déclarations conditionnelles fournies dans cette section.]

a) Il faut laver la voiture du boss pour être promu.

b) Les vents du sud impliquent un dégel printanier.

c) Une condition suffisante pour que la garantie soit valable est que vous avez acheté l'ordinateur il y a moins d'un an.

d) Willy se fait prendre chaque fois qu'il triche.

e) Vous ne pouvez accéder au site Web que si vous payez un abonnement frais de dossier.

f) Être élu découle de la connaissance des bonnes personnes ple.

g) Carol a le mal de mer quand elle est sur un bateau.

23. Écrivez chacune de ces déclarations sous la forme «si p , alors q » en anglais. [*Astuce:* reportez - vous à la liste des moyens courants exprimer des déclarations conditionnelles.]

a) Il neige chaque fois que le vent souffle du nord-est.

b) Les pommiers fleuriront s'il reste chaud pendant une semaine.

c) Que les Pistons remportent le championnat implique que ils ont battu les Lakers.

d) Il faut marcher 8 milles pour arriver au sommet de Pic de Long.

e) Pour obtenir la permanence en tant que professeur, il suffit d'être célèbre.

f) Si vous conduisez plus de 400 miles, vous devrez acheter de l'essence.

g) Votre garantie n'est valable que si vous avez acheté votre CD joueur il y a moins de 90 jours.

h) Jan ira nager à moins que l'eau ne soit trop froide.

24. Écrivez chacune de ces déclarations sous la forme «si p , alors q » en anglais. [*Astuce:* reportez - vous à la liste des moyens courants presse les déclarations conditionnelles fournies dans cette section.]

a) Je n'oublierai de vous envoyer l'adresse que si vous envoyez-moi un e-mail.

b) Pour être citoyen de ce pays, il suffit que vous sont nés aux États-Unis.

c) Si vous conservez votre manuel, ce sera une référence utile dans vos futurs cours.

d) Les Red Wings gagneront la Coupe Stanley si leur gardien de but joue bien.

e) Que vous obteniez le travail implique que vous aviez le meilleur identifiants.

f) La plage s'érode en cas de tempête.

g) Il est nécessaire d'avoir un mot de passe valide pour se connecter le serveur.

h) Vous atteindrez le sommet à moins de commencer votre ascension trop tard.

25. Écrivez chacune de ces propositions sous la forme « p si et uniquement si q "en anglais.

a) S'il fait chaud dehors, vous achetez un cornet de crème glacée et si vous achetez un cornet de crème glacée il fait chaud dehors.

b) Pour que vous puissiez gagner le concours, il est nécessaire et suffisant que vous avez le seul ticket gagnant.

c) Vous êtes promu uniquement si vous avez des connexions, et vous avez des connexions uniquement si vous êtes promu.

d) Si vous regardez la télévision, votre esprit se décomposera et vers.

e) Les trains arrivent en retard exactement les jours où je prends il.

26. Écrivez chacune de ces propositions sous la forme « p si et uniquement si q "en anglais.

a) Pour obtenir un A dans ce cours, il est nécessaire et suffit d'apprendre à résoudre des mathématiques discrètes

c) $q \lor p \lor \neg s \lor \neg r \lor \neg t \lor u$

d) $(p \land r \land t) \leftrightarrow (q \land t)$

30. Combien de lignes apparaissent dans une table de vérité pour chacune de ces propositions composées?

a) $(q \to \neg p) \lor (\neg p \to \neg q)$

b) $(p \lor \neg t) \land (p \lor \neg s)$

c) $(p \to r) \lor (\neg s \to \neg t) \lor (\neg u \to v)$

d) $(p \land r \land s) \lor (q \land t) \lor (r \land \neg t)$

31. Construisez une table de vérité pour chacune de ces propositions composées. sitions.

a) $p \land \neg p$ **b)** $p \lor \neg p$

c) $(p \lor \neg q) \to q$ **d)** $(p \lor q) \to (p \land q)$

e) $(p \to q) \leftrightarrow (\neg q \to \neg p)$

f) $(p \to q) \to (q \to p)$

32. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $p \to \neg p$ **b)** $p \leftrightarrow \neg p$

c) $p \oplus (p \lor q)$ **d)** $(p \land q) \to (p \lor q)$

e) $(q \to \neg p) \leftrightarrow (p \leftrightarrow q)$

f) $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$

33. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $(p \lor q) \to (p \oplus q)$ **b)** $(p \oplus q) \to (p \land q)$

c) $(p \lor q) \oplus (p \land q)$ **d)** $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow q)$

e) $(p \leftrightarrow q) \oplus (\neg p \leftrightarrow \neg r)$

f) $(p \oplus q) \to (p \oplus \neg q)$

34. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $p \oplus p$ **b)** $p \oplus \neg p$

c) $p \oplus \neg q$ **d)** $\neg p \oplus \neg q$

e) $(p \oplus q) \lor (p \oplus \neg q)$ **f)** $(p \oplus q) \land (p \oplus \neg q)$

problèmes matiques.

b) Si vous lisez le journal tous les jours, vous serez formé, et inversement.

c) Il pleut si c'est un jour de week-end, et c'est un jour de week-end s'il pleut.

d) Vous ne pouvez voir l'assistant que s'il n'est pas dans, et l'assistant n'est pas seulement si vous pouvez le voir.

27. Énoncez l'inverse, la contraposition et l'inverse de chacun des ces déclarations conditionnelles.

a) S'il neige aujourd'hui, je skierai demain.

b) Je viens en classe chaque fois qu'il y aura un quiz.

c) Un entier positif n'est un nombre premier que s'il n'a pas de diviseurs autre que 1 et lui-même.

28. Énoncez l'inverse, la contraposition et l'inverse de chacun des ces déclarations conditionnelles.

a) S'il neige ce soir, je resterai à la maison.

b) Je vais à la plage chaque fois que c'est une journée d'été ensoleillée.

c) Quand je me lève tard, il faut que je dorme jusqu'à le midi.

29. Combien de lignes apparaissent dans une table de vérité pour chacune de ces propositions composées?

a) $p \to \neg p$

b) $(p \vee \neg r) \wedge (q \vee \neg s)$

35. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $p \to \neg q$ **b)** $\neg p \leftrightarrow q$

c) $(p \to q) \vee (\neg p \to q)$ **d)** $(p \to q) \wedge (\neg p \to q)$

e) $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$

f) $(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$

36. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $(p \vee q) \vee r$ **b)** $(p \vee q) \wedge r$

c) $(p \wedge q) \vee r$ **d)** $(p \wedge q) \wedge r$

e) $(p \vee q) \wedge \neg r$ **f)** $(p \wedge q) \vee \neg r$

37. Construisez une table de vérité pour chacune de ces propositions sitions.

a) $p \to (\neg q \vee r)$

b) $\neg p \to (q \to r)$

c) $(p \to q) \vee (\neg p \to r)$

d) $(p \to q) \wedge (\neg p \to r)$

e) $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$

f) $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$

38. Construisez une table de vérité pour $((p \to q) \to r) \to s$.

39. Construire une table de vérité pour $(p \leftrightarrow q) \leftrightarrow (r \leftrightarrow s)$.

40. Expliquez, sans utiliser de table de vérité, pourquoi $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ est vrai lorsque p , q et r ont la valeur même valeur de vérité et c'est faux sinon.

41. Expliquez, sans utiliser de table de vérité, pourquoi $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ est vrai quand au moins l'un de p , q et r est vrai et au moins un est faux, mais est faux lorsque les trois les variables ont la même valeur de vérité.

42. Quelle est la valeur de x après chacun de ces énoncés est rencontré dans un programme informatique, si $x = 1$ avant la déclaration est atteinte?

a) si $x + 2 = 3$ **alors** $x := x + 1$

b) si $(x + 1 = 3)$ OU $(2x + 2 = 3)$ **alors** $x := x + 1$

c) si $(2x + 3 = 5)$ ET $(3x + 4 = 7)$ **alors** $x := x + 1$

d) si $(x + 1 = 2)$ XOR $(x + 2 = 3)$ **alors** $x := x + 1$

e) si $x < 2$ **alors** $x := x + 1$

43. Trouvez le bit à bit OU , bit à bit ET et bit à bit XOR de chacune de ces paires de chaînes de bits.

a) 101 1110 , 010 0001

b) 1111 0000 , 1010 1010

c) 00 0111 0001 , 10 0100 1000

d) 11 1111 1111 , 00 0000 0000

44. Évaluez chacune de ces expressions.

a) $1\,1000 \wedge (0\,1011 \vee 1\,1011)$

b) $(0\,1111 \wedge 1\,0101) \vee 0\,1000$

c) $(0\,1010 \oplus 1\,1011) \oplus 0\,1000$

d) $(1\,1011 \vee 0\,1010) \wedge (1\,0001 \vee 1\,1011)$

La logique floue est utilisée en intelligence artificielle. En logique floue, un proposition a une valeur de vérité qui est un nombre compris entre 0 et 1, compris. Une proposition avec une valeur de vérité de 0 est fausse et une avec une valeur de vérité de 1 est vrai. Valeurs de vérité comprises entre 0 et 1 indiquent divers degrés de vérité. Par exemple, la vérité la valeur 0,8 peut être affectée à la déclaration «Fred est heureux» parce que Fred est heureux la plupart du temps, et la valeur de la vérité 0,4 peut être attribué à la déclaration «John est heureux», car John est content un peu moins de la moitié du temps. Utilisez ces vérités valeurs à résoudre Exercices 45–47.

45. La valeur de vérité de la négation d'une proposition en flou la logique est 1 moins la valeur de vérité de la proposition. Quoi sont les valeurs de vérité des déclarations «Fred n'est pas content» et "John n'est pas content?"

46. La valeur de vérité de la conjonction de deux propositions dans la logique floue est le minimum des valeurs de vérité des deux propositions. Quelles sont les valeurs de vérité des déclarations "Fred et John sont heureux" et "Ni Fred ni John ne sont content?"

47. La valeur de vérité de la disjonction de deux propositions dans la logique floue est le maximum des valeurs de vérité des deux propositions. Quelles sont les valeurs de vérité des déclarations "Fred est heureux, ou John est heureux" et "Fred n'est pas heureux, ou John n'est pas content? "

* **48.** L'affirmation «Cette affirmation est fausse» est-elle une proposition?

* **49.** Le n ième instruction dans une liste de 100 déclarations est « Exactement n des déclarations de cette liste sont fausses. »

a) Quelles conclusions pouvez-vous tirer de ces déclarations ments?

b) une partie de réponse (a) si la n ième déclaration est « au moins n de les déclarations de cette liste sont fausses. »

c) Répondez à la partie (b) en supposant que la liste contient 99 déclarations.

50. Une ancienne légende sicilienne dit que le barbier dans une télécommande ville qui ne peut être atteint que par un voyage dangereux route de montagne rase ces gens, et seuls ceux qui des gens qui ne se rasent pas. Peut-il y avoir un tel coiffeur?

Applications de la logique propositionnelle

introduction

La logique a de nombreuses applications importantes en mathématiques, en informatique et dans de nombreux autres disciplines. Les énoncés en mathématiques et en sciences et en langage naturel sont souvent imprécis ou ambigu. Pour que ces déclarations soient précises, elles peuvent être traduites dans la langue de la logique. Par exemple, la logique est utilisée dans la spécification des logiciels et du matériel, car ces les spécifications doivent être précises avant le début du développement.De plus, la logique propositionnelle et ses règles peuvent être utilisées pour concevoir des circuits informatiques, pour construire des programmes informatiques, pour vérifier l'exactitude des programmes et de construire des systèmes experts.La logique peut être utilisée pour analyser et résoudre de nombreux puzzles familiers. Des systèmes logiciels basés sur les règles de la logique ont été développés pour construire automatiquement certains types de preuves, mais pas tous.Nous allons discuter de certains de ces applications de la logique propositionnelle dans cette section et dans les chapitres suivants.

Traduction des phrases en anglais

Il existe de nombreuses raisons de traduire des phrases anglaises en expressions impliquant des propositions variables et connecteurs logiques. En particulier, l'anglais (et toutes les autres langues humaines) est

souvent ambigu. Traduire des phrases en déclarations composées (et autres types de logique expressions, que nous présenterons plus loin dans ce chapitre) supprime l'ambiguïté. Notez que cela peut impliquer de faire un ensemble d'hypothèses raisonnables fondées sur la signification phrase. De plus, une fois que nous avons traduit des phrases de l'anglais en expressions logiques nous pouvons analyser ces expressions logiques pour déterminer leurs valeurs de vérité, nous pouvons manipuler eux, et nous pouvons utiliser des règles d'inférence (qui sont discutées dans la section 1.6) pour raisonner sur leur.

Pour illustrer le processus de traduction d'une phrase anglaise en une expression logique, considérez Exemples 1 et 2.

EXEMPLE 1 Comment traduire cette phrase anglaise en une expression logique?

"Vous ne pouvez accéder à Internet à partir du campus que si vous êtes majeur en informatique ou si ne sont pas des étudiants de première année. "

Solution: Il existe de nombreuses façons de traduire cette phrase en une expression logique.Bien qu'il soit possible de représenter la phrase par une seule variable propositionnelle, telle que p , ce ne serait pas utile pour analyser sa signification ou son raisonnement. Au lieu de cela, nous utiliserons des variantes propositionnelles capable de représenter chaque partie de phrase et de déterminer les connecteurs logiques appropriés entre leur. En particulier, nous laissons a , c et f représenter «Vous pouvez accéder à Internet depuis le campus» «Vous êtes un majeur en informatique» et «Vous êtes un étudiant de première année», respectivement.Notant que «seulement si »est une façon d'exprimer une déclaration conditionnelle, cette phrase peut être représentée comme

$$a \to (c \vee \neg f).$$ ▲

EXEMPLE 2 Comment traduire cette phrase anglaise en une expression logique?

«Vous ne pouvez pas monter sur les montagnes russes si vous mesurez moins de 4 pieds, sauf si vous avez plus de 16 ans ans."

Solution: Soit q , r et s représentent «Vous pouvez monter sur les montagnes russes», «Vous mesurez moins de 4 pieds» et "Vous avez plus de 16 ans", respectivement. Ensuite, la phrase peut être traduite en

$$(r \wedge \neg s) \to \neg q.$$

Bien sûr, il existe d'autres façons de représenter la phrase d'origine comme une expression logique, mais celui que nous avons utilisé devrait répondre à nos besoins. ▲

Spécifications du système

La traduction de phrases en langage naturel (comme l'anglais) en expressions logiques est un élément essentiel partie de la spécification des systèmes matériels et logiciels.Les ingénieurs système et logiciels prennent exigences en langage naturel et produire des spécifications précises et sans ambiguïté qui peuvent être utilisé comme base pour le développement du système.L'exemple 3 montre comment les propositions composées peut être utilisé dans ce processus.

EXEMPLE 3 Exprimer la spécification «La réponse automatisée ne peut pas être envoyée lorsque le système de fichiers est plein» en utilisant des connecteurs logiques.

Solution: Une façon de traduire ceci est de laisser p indiquer «La réponse automatisée peut être envoyée» et q indique "Le système de fichiers est plein". Alors $\neg p$ représente "Il n'est pas vrai que l'automatisation réponse peut être envoyée », qui peut également être exprimée par« La réponse automatisée ne peut pas être envoyée ». Par conséquent, notre spécification peut être représentée par l'instruction conditionnelle $q \rightarrow \neg p$. ▲

Les spécifications du système doivent être **cohérentes** , c'est-à-dire qu'elles ne doivent pas contenir de conflits exigences qui pourraient être utilisées pour dériver une contradiction. Lorsque les spécifications ne sont pas cohérentes, il n'y aurait aucun moyen de développer un système qui satisfasse à toutes les spécifications.

EXEMPLE 4 Déterminez si ces spécifications système sont cohérentes:

"Le message de diagnostic est stocké dans le tampon ou il est retransmis."
"Le message de diagnostic n'est pas stocké dans le tampon."
"Si le message de diagnostic est stocké dans le tampon, il est retransmis."

Solution: Pour déterminer si ces spécifications sont cohérentes, nous les exprimons d'abord en utilisant expressions logiques. Soit p dénoté "Le message de diagnostic est stocké dans le tampon" et soit q dénoter «Le message de diagnostic est retransmis». Les spécifications peuvent alors être écrites $p \vee q$, $\neg p$ et $p \rightarrow q$. Une affectation de valeurs de vérité qui rend les trois spécifications vraies doit avoir p false pour rendre $\neg p$ vrai. Parce que nous voulons que $p \vee q$ soit vrai mais p doit être faux, q doit être vrai. Parce que $p \rightarrow q$ est vrai lorsque p est faux et q est vrai, nous concluons que ces les spécifications sont cohérentes, car elles sont toutes vraies lorsque p est faux et q est vrai. Nous pourrions arriver à la même conclusion en utilisant une table de vérité pour examiner les quatre affectations possibles des valeurs de vérité à p et q . ▲

EXEMPLE 5 Les spécifications du système de l'exemple 4 restent-elles cohérentes si la spécification «Le diagnostic message n'est pas retransmis »est ajouté?

Solution: selon le raisonnement de l'exemple 4, les trois spécifications de cet exemple sont vraies uniquement dans le cas où p est faux et q est vrai. Cependant, cette nouvelle spécification est $\neg q$, ce qui est false lorsque q est vrai. Par conséquent, ces quatre spécifications sont incohérentes. ▲

Recherches booléennes

Les connecteurs logiques sont largement utilisés dans les recherches de grandes collections d'informations, telles que comme index de pages Web. Parce que ces recherches utilisent des techniques de logique propositionnelle, ce sont **des recherches booléennes** .

Dans les recherches booléennes, le connecteur *ET* est utilisé pour faire correspondre les enregistrements contenant à la fois deux termes de recherche, le *OU* conjonctif est utilisé pour faire correspondre l'un ou les deux termes de recherche, et le le connectif *NOT* (parfois écrit *ET ET NON*) est utilisé pour exclure un terme de recherche particulier. Une planification minutieuse de l'utilisation des connecteurs logiques est souvent requise lors des recherches booléennes sont utilisés pour localiser des informations d'intérêt potentiel. L'exemple 6 illustre comment les recherches booléennes sont effectués.

EXEMPLE 6 **Recherche de pages Web La** plupart des moteurs de recherche Web prennent en charge les techniques de recherche booléenne, qui peut généralement aider à trouver des pages Web sur des sujets particuliers. Par exemple, en utilisant la recherche booléenne pour trouver des pages Web sur les universités au Nouveau-Mexique, nous pouvons rechercher des pages correspondant à NOUVEAU *ET* MEXIQUE *ET* UNIVERSITÉS. Les résultats de cette recherche incluront les pages qui contiennent les trois mots NEW, MEXICO et UNIVERSITIES.Cela comprendra tous les pages d'intérêt, ainsi que d'autres telles qu'une page sur les nouvelles universités au Mexique.(Remarque que dans Google et dans de nombreux autres moteurs de recherche, le mot "ET" n'est pas nécessaire, compris, car tous les termes de recherche sont inclus par défaut. Ces moteurs de recherche prennent également en charge l'utilisation de guillemets pour rechercher des expressions spécifiques. Ainsi, il peut être plus efficace de rechercher pour les pages correspondant à "Nouveau Mexique" *ET* UNIVERSITÉS.)

Ensuite, pour trouver des pages qui traitent des universités au Nouveau-Mexique ou en Arizona, nous pouvons rechercher pour les pages correspondant (NOUVEAU *ET* MEXIQUE *OU* ARIZONE) *ET* UNIVERSITÉS. (*Remarque:* ici l' opérateur *AND* a priorité sur l' opérateur *OR* . De plus, dans Google, les termes utilisés pour cette recherche serait NOUVEAU MEXIQUE *OU* ARIZONE.) Les résultats de cette recherche incluront toutes les pages qui contiennent le mot UNIVERSITIES et les mots NEW et MEXICO ou le mot ARIZONA. Encore une fois, des pages autres que celles qui vous intéressent seront répertoriées. Enfin, pour trouver Les pages Web qui traitent des universités au Mexique (et non au Nouveau-Mexique), nous pourrions d'abord regarder pour les pages correspondant au MEXIQUE *ET* AUX UNIVERSITÉS, mais parce que les résultats de cette recherche inclure des pages sur les universités au Nouveau-Mexique, ainsi que les universités au Mexique, il pourrait être mieux pour rechercher des pages correspondant (MEXIQUE *ET* UNIVERSITÉS) *PAS* NOUVEAU. Les resultats de cette recherche comprennent des pages qui contiennent à la fois les mots MEXIQUE et UNIVERSITÉS mais ne contiennent pas le mot NOUVEAU.(Dans Google et dans de nombreux autres moteurs de recherche, le mot "NON" est remplacé par le symbole «-». Dans Google, les termes utilisés pour cette dernière recherche seraient MEXIQUE UNIVERSITÉS -NOUVEAU.) ▲

Puzzles logiques

Les puzzles qui peuvent être résolus en utilisant le raisonnement logique sont appelés **puzzles logiques** . Logique de résolution puzzles est un excellent moyen de s'entraîner à travailler avec les règles de la logique.Aussi, les programmes informatiques conçus pour effectuer un raisonnement logique utilisent souvent des puzzles logiques bien connus pour illustrer leur capacités. Beaucoup de gens aiment résoudre des énigmes logiques, publiées dans des périodiques, des livres et sur le Web, comme activité récréative.

Nous allons discuter ici de deux énigmes logiques.Nous commençons par un puzzle posé à l'origine par Raymond Smullyan, un maître des puzzles de logique, qui a publié plus d'une douzaine de livres contenant des puzzles difficiles qui impliquent un raisonnement logique.Dans la section 1.3, nous discuterons également puzzle logique extrêmement populaire Sudoku.

EXEMPLE 7 Dans [Sm78] Smullyan a posé de nombreuses énigmes sur une île qui a deux types d'habitants, les chevaliers, qui disent toujours la vérité, et leurs opposés, les chevaliers, qui mentent toujours.Vous rencontrez deux personnes A et B . Que sont A et B si A dit « B est un chevalier» et B dit «Nous sommes tous les deux types opposés? "

Solution: Soit p et q les déclarations que A est un chevalier et B est un chevalier, respectivement, de sorte que $\neg p$ et $\neg q$ sont les déclarations que A est un knave et B est un knave, respectivement.

Nous considérons d'abord la possibilité que A soit un chevalier; c'est l'affirmation que p est vrai. Si A est un chevalier, puis il dit la vérité quand il dit que B est un chevalier, de sorte que q est vrai, et A et B sont du même type. Cependant, si B est un chevalier, alors la déclaration de B selon laquelle A et B sont de types, l'énoncé $(p \wedge \neg q) \vee (\neg p \wedge q)$, devrait être vrai, ce qui n'est pas le cas, car A et B sont tous deux chevaliers. Par conséquent, nous pouvons conclure que A n'est pas un chevalier, c'est-à-dire que p est faux.

Si A est un knave, alors parce que tout ce qu'un knave dit est faux, la déclaration de A selon laquelle B est un chevalier, c'est-à-dire que q est vrai, est un mensonge.Cela signifie que q est faux et B est également un valet. De plus, si B est un valet, alors la déclaration de B selon laquelle A et B sont des types opposés est un mensonge, ce qui est cohérent avec A et B étant des fripons. Nous pouvons conclure que A et B sont tous les deux fripons. ▲

Nous posons plus d'énigmes de Smullyan sur les chevaliers et les chevaliers dans les Exercices 19-23Dans Les exercices 24 à 31 présentent des énigmes connexes où nous avons trois types de personnes, des chevaliers et des des fripons comme dans ce puzzle avec des espions qui peuvent mentir.

Ensuite, nous posons un puzzle connu sous le nom de **puzzle d'enfants boueux** pour le cas de deux enfants.

EXEMPLE 8 Un père dit à ses deux enfants, un garçon et une fille, de jouer dans leur jardin sans se salir. Cependant, en jouant, les deux enfants ont de la boue sur le front. Quand les enfants s'arrêtent en jouant, le père dit "Au moins l'un d'entre vous a le front boueux", puis demande aux enfants pour répondre «Oui» ou «Non» à la question: «Savez-vous si vous avez le front boueux?» Le père pose cette question deux fois. À quoi les enfants répondront-ils à chaque fois que cette question demandé, en supposant qu'un enfant peut voir si son frère a le front boueux, mais ne peut pas voir son propre front? Supposons que les deux enfants sont honnêtes et que les enfants répondent chaque question simultanément.

Solution: Soit s soit la déclaration que le fils a un front boueux et laisser d la déclaration la fille a le front boueux. Quand le père dit qu'au moins un des deux enfants a le front boueux, il déclare que la disjonction $s \vee d$ est vraie. Les deux enfants répondront «Non» la première fois que la question est posée car chacun voit de la boue sur le front de l'autre enfant. Autrement dit, le fils sait que d est vrai, mais ne sait pas si s est vrai, et la fille sait que s est vrai, mais ne sait pas si d est vrai.

Après que le fils a répondu «Non» à la première question, la fille peut déterminer que d doit être vrai. Cela suit parce que lorsque la première question est posée, le fils sait que $s \vee d$ est vrai, mais ne peut pas déterminer si s est vrai. En utilisant ces informations, la fille peut conclure que d doit être vrai, car si d était faux, le fils aurait pu raisonner parce que $s \vee d$ est vrai, alors s doit être vrai, et il aurait répondu «Oui» à la première question. Le fils peut raisonner de manière similaire pour déterminer que s doit être vrai. Il s'ensuit que les deux enfants répondent «oui» au deuxième fois la question est posée. ▲

Circuits logiques

La logique propositionnelle peut être appliquée à la conception de matériel informatique. Cela a d'abord été observé en 1938 par Claude Shannon dans sa thèse de maîtrise du MIT. Dans le chapitre 12, nous étudierons ce sujet en profondeur. (Voir ce chapitre pour une biographie de Shannon.) Nous donnons une brève introduction à ce application ici.

Un **circuit logique** (ou **circuit numérique**) reçoit les signaux d'entrée $p_1, p_2, ..., p_n$, chacun un bit [soit 0 (désactivé) ou 1 (activé)], et produit des signaux de sorties $s_1, s_2, ..., s_n$, chacun un peu. Dans cette section, nous allons restreindre notre attention aux circuits logiques avec un seul signal de sortie; en général, les circuits numériques peuvent avoir plusieurs sorties.

Au chapitre 12, nous concevons quelques circuits utiles.

RAYMOND SMULLYAN (NÉ EN 1919) Raymond Smullyan a abandonné ses études secondaires. Il voulait étudier ce qui l'intéressait vraiment et non le matériel standard du secondaire. Après avoir sauté d'une université à le lendemain, il a obtenu un diplôme de premier cycle en mathématiques à l'Université de Chicago en 1955. Il a payé ses dépenses de collège en effectuant des tours de magie dans les fêtes et les clubs. Il a obtenu un doctorat. en logique en 1959 à Princeton, étudiant sous Alonzo Church. Après avoir obtenu son diplôme de Princeton, il a enseigné les mathématiques et la logique à Dartmouth College, Princeton University, Yeshiva University et City University of New York. Il a rejoint le département de philosophie de l'Université d'Indiana en 1981 où il est maintenant professeur émérite.

Smullyan a écrit de nombreux livres sur la logique récréative et les mathématiques, notamment *Satan, Cantor et Infini; Quel est le nom de ce livre?; La Dame ou le tigre ?; Alice dans Puzzleland; Se moquer d'un oiseau moqueur; Toujours indécis;* et *L'énigme de Scheherazade: énigmes logiques étonnantes, anciennes et modernes* . Parce que ses énigmes logiques sont stimulant, divertissant et stimulant, il est considéré comme un Lewis Carroll moderne. Smullyan a également écrit plusieurs livres sur l'application de la logique déductive aux échecs, trois recueils d'essais philosophiques et d'aphorismes, et plusieurs livres avancés sur la logique mathématique et la théorie des ensembles. Il s'intéresse particulièrement à l'auto-référence et a travaillé sur l'extension certains des résultats de Gödel qui montrent qu'il est impossible d'écrire un programme informatique capable de résoudre tous les problèmes mathématiques. Il est particulièrement intéressé à expliquer au public les idées de la logique mathématique.

Smullyan est un musicien talentueux et joue souvent du piano avec sa femme, pianiste de niveau concert. La fabrication de télescopes en est une de ses hobbies. Il s'intéresse également à l'optique et à la photographie stéréo. Il déclare: «Je n'ai jamais eu de conflit entre l'enseignement et la recherche comme le font certaines personnes parce que quand j'enseigne, je fais de la recherche. »Smullyan fait l'objet d'un court métrage documentaire intitulé *Ce film n'a pas besoin de titre* .

p $\neg p$ p q $p \vee q$ p q $p \wedge q$

Onduleur Porte OU ET porte

FIGURE 1 **Portes logiques de base.**

p $p \wedge \neg q$
q $(p \wedge \neg q) \vee \neg r$
$\neg q$
r
$\neg r$

FIGURE 2 **Un circuit combinatoire.**

Les circuits numériques compliqués peuvent être construits à partir de trois circuits de base, appelés **portes** , illustrés sur la figure 1. L' **onduleur** , ou **porte NON** , prend un bit d'entrée p et produit comme sortie $\neg p$. le **La porte OU** prend deux signaux d'entrée p et q , chacun un peu, et produit en sortie le signal $p \vee q$. Enfin, la **porte ET** prend deux signaux d'entrée p et q , chacun un peu, et produit en sortie le signal $p \wedge q$. Nous utilisons des combinaisons de ces trois portes de base pour construire des circuits plus compliqués, comme celle illustrée à la figure 2.

Étant donné un circuit construit à partir des portes logiques de base et des entrées du circuit, nous déterminons la sortie en traçant à travers le circuit, comme le montre l'exemple 9.

EXEMPLE 9 Déterminez la sortie du circuit combinatoire de la figure 2.

Solution: sur la figure 2, nous affichons la sortie de chaque porte logique du circuit.Nous voyons que le ET la grille prend l'entrée de p et $\neg q$, la sortie de l'onduleur avec l'entrée q , et produit $p \wedge \neg q$. On note ensuite que la porte OU prend les entrées $p \wedge \neg q$ et $\neg r$, la sortie de l'onduleur avec entrée r , et produit la sortie finale $(p \wedge \neg q) \vee \neg r$. ▲

Supposons que nous ayons une formule pour la sortie d'un circuit numérique en termes de négations, disjonctions et conjonctions. Ensuite, nous pouvons systématiquement construire un circuit numérique avec le sortie souhaitée, comme illustré dans l'exemple 10.

EXEMPLE 10 Construire un circuit numérique qui produit la sortie $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$ lorsqu'une entrée est donnée bits p , q et r .

Solution: Pour construire le circuit souhaité, nous construisons des circuits séparés pour $p \vee \neg r$ et pour $\neg p \vee (q \vee \neg r)$ et combinez-les à l'aide d'une porte ET. Pour construire un circuit pour $p \vee \neg r$, on utilise un inverseur pour produire $\neg r$ *à* partir de l'entrée r . Ensuite, nous utilisons une porte OU pour combiner p et $\neg r$. À construire un circuit pour $\neg p \vee (q \vee \neg r)$, on utilise d'abord un inverseur pour obtenir $\neg r$. Ensuite, nous utilisons une porte OU avec les entrées q et $\neg r$ pour obtenir $q \vee \neg r$. Enfin, nous utilisons un autre onduleur et une porte OU pour obtenir $\neg p \vee (q \vee \neg r)$ des entrées p et $q \vee \neg r$.

Pour terminer la construction, nous utilisons une porte ET finale, avec les entrées $p \vee \neg r$ et $\neg p \vee (q \vee \neg r)$. Le circuit résultant est affiché à la figure 3. ▲

Nous étudierons en détail les circuits logiques au chapitre 12 dans le contexte de l'algèbre de Boole, et avec une notation différente.

p $p \vee \neg r$
r
$\neg r$ $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$
$\neg p$
p
q $\neg p \vee (q \vee \neg r)$
r $q \vee \neg r$
$\neg r$

FIGURE 3 **Le circuit pour $(p \vee \neg r) \wedge (\neg p \vee (q \vee \neg r))$.**

Des exercices

Dans les exercices 1 à 6, traduisez la déclaration donnée en proposi-
logique logique en utilisant les propositions fournies.

1. Vous ne pouvez pas modifier une entrée Wikipédia protégée à moins êtes administrateur. Exprimez votre réponse en termes de *e* : "Vous pouvez modifier une entrée Wikipédia protégée" et *un* : "Vous êtes un administrateur. "

2. Vous pouvez voir le film uniquement si vous avez plus de 18 ans ou vous avez la permission d'un parent. Exprimez votre swer en termes de *m* : "Vous pouvez voir le film", *e* : "Vous êtes de plus de 18 ans »et *p* :« Vous avez la permission d'un parent."

3. Vous ne pouvez obtenir votre diplôme que si vous avez rempli de votre commandant et vous ne devez pas d'argent au l'université et vous n'avez pas un livre de bibliothèque en retard. Exprimez votre réponse en termes de *g* : «Vous pouvez obtenir votre diplôme» *m* : «Vous devez de l'argent à l'université», *r* : «Vous avez satisfait aux exigences de votre majeure », et *b* :« Vous avez un livre de bibliothèque en retard. "

4. Pour utiliser le réseau sans fil de l'aéroport, vous devez payer les frais journaliers, sauf si vous êtes abonné au service. Exprimez votre réponse en termes de *w* : «Vous pouvez utiliser le moins de réseau dans l'aéroport ", *d* :" Vous payez les frais quotidiens ", et *s* : "Vous êtes abonné au service."

5. Vous ne pouvez être président des États-Unis que si vous sont âgés d'au moins 35 ans, sont nés aux États-Unis ou au moment de votre naissance, vos deux parents étaient citoyens, et vous avez vécu au moins 14 ans dans le pays. Express votre réponse en termes de *e* : «Vous êtes éligible pour être ident of the USA », *a* :« Vous avez au moins 35 ans » *b* : «Vous êtes né aux États-Unis», *p* : «Au moment de votre naissance, vos deux parents où les citoyens, "et *r* :" Vous ont vécu au moins 14 ans aux USA »

6. Vous ne pouvez mettre à niveau votre système d'exploitation que si vous avez un processeur 32 bits fonctionnant à 1 GHz ou plus, au moins 1 Go de RAM et 16 Go d'espace libre sur le disque dur, ou un 64- processeur binaire fonctionnant à 2 GHz ou plus, au moins 2 Go RAM et au moins 32 Go d'espace libre sur le disque dur. Express vous répondez en termes de *u* : «Vous pouvez mettre à niveau votre système d'exploitation », b_{32} :« Vous avez un processeur 32 bits », b_{64} : «Vous avez un processeur 64 bits», g_1 : «Votre processeur fonctionne à 1 GHz ou plus rapide, " g_2 :" Votre processeur fonctionne à 2 GHz ou plus rapide », r_1 :« Votre processeur possède au moins 1 Go de RAM », r_2 : "Votre processeur a au moins 2 Go de RAM", h_{16} : "Vous avez au moins 16 Go d'espace libre sur le disque dur ", et h_{32} :" Vous avez au moins 32 Go d'espace libre sur le disque dur. "

7. Exprimez ces spécifications du système en utilisant la tions *p* « Le message est analysé pour les virus » et *q* « La message a été envoyé à partir d'un système inconnu "ensemble avec des connecteurs logiques (y compris les négations).

a) «Le message est analysé pour détecter les virus à chaque message a été envoyé à partir d'un système inconnu. "

b) «Le message a été envoyé depuis un système inconnu mais il n'a pas été analysé pour les virus. "

c) «Il est nécessaire de rechercher des virus dans le message lorsque-jamais il a été envoyé à partir d'un système inconnu. "

d) «Lorsqu'un message n'est pas envoyé depuis un système inconnu il n'est pas analysé pour les virus. "

8. Exprimez ces spécifications du système en utilisant la tions *p* « L'utilisateur entre un mot de passe valide, » *q* « L' accès est accordé "et *r* " L'utilisateur a payé les frais d'abonnement " et les connecteurs logiques (y compris les négations).

a) «L'utilisateur a payé les frais d'abonnement, mais ne entrez un mot de passe valide. "

b) «L'accès est accordé chaque fois que l'utilisateur a payé frais d'abonnement et saisit un mot de passe valide. "

c) «L'accès est refusé si l'utilisateur n'a pas payé l'abonnement frais de publication. "

d) «Si l'utilisateur n'a pas entré de mot de passe valide mais a payé les frais d'abonnement, puis l'accès est accordé. "

9. Ces spécifications système sont-elles cohérentes? "Le système est en état multi-utilisateur si et seulement s'il fonctionne normalement. Si le système fonctionne normalement, le noyau fonctionne tionnement. Le noyau ne fonctionne pas ou le système est en mode interruption. Si le système n'est pas en état multi-utilisateur, il est alors en mode interruption. Le système n'est pas en interruption mode."

10. Ces spécifications système sont-elles cohérentes? "N'importe quand le logiciel système est en cours de mise à niveau, les utilisateurs ne quitter le système de fichiers. Si les utilisateurs peuvent accéder au système de fichiers, ils peuvent alors enregistrer de nouveaux fichiers. Si les utilisateurs ne peuvent pas enregistrer de nouveaux fichiers, le logiciel système n'est pas mis à niveau. "

11. Ces spécifications système sont-elles cohérentes? «Le routeur peut envoyer des paquets au système de périphérie que s'il prend en charge nouvel espace d'adressage. Pour que le routeur prenne en charge la nouvelle habiller l'espace, il est nécessaire que la dernière version du logiciel être installé. Le routeur peut envoyer des paquets au système de périphérie si la dernière version du logiciel est installée, le routeur ne prend pas en charge le nouvel espace d'adressage. »

12. Ces spécifications système sont-elles cohérentes? "Si le fichier le système n'est pas verrouillé, les nouveaux messages seront mis en file d'attente. Si le système de fichiers n'est pas verrouillé, alors le système fonctionne normalement et inversement. Si de nouveaux messages ne sont pas en file d'attente, puis ils seront envoyés au tampon de messages. Si le système de fichiers n'est pas verrouillé, alors de nouveaux messages seront envoyé au tampon de messages. Aucun nouveau message ne sera envoyé au tampon de messages. "

13. Quelle recherche booléenne utiliseriez-vous pour rechercher le Web pages sur les plages du New Jersey? Et si tu voulais pour trouver des pages Web sur les plages de l'île de Jersey (en La Manche)?

14. Quelle recherche booléenne utiliseriez-vous pour rechercher le Web pages sur la randonnée en Virginie-Occidentale? Et si tu voulais pour trouver des pages Web sur la randonnée en Virginie, mais pas dans l'Ouest Virginie?

* **15.** Chaque habitant d'un village isolé dit toujours la vérité ou ment toujours. Un villageois ne donnera qu'un «oui» ou un «non» réponse à une question posée par un touriste. Supposons que vous soyez touriste visitant cette région et venir à une bifurcation de la route.

devenir malheureux si Samir est là, Samir assistera seulement si Kanti sera là, et Kanti ne sera pas présent à moins que Jas- bien aussi. Quelles combinaisons de ces trois amis pouvez-vous inviter pour ne pas rendre quelqu'un malheureux?

Les exercices 19-23 concernent les habitants de l'île des chevaliers et les nègres créés par Smullyan, où les chevaliers disent toujours la vérité et les fripons mentent toujours. Vous rencontrez deux personnes, *A* et *B* . Déterminez, si possible, ce que sont *A* et *B* s'ils vous adresser de la manière décrite. Si vous ne pouvez pas déterminer quelles sont ces deux personnes, pouvez-vous tirer des conclusions?

19. *A* dit «Au moins l'un d'entre nous est un coquin» et *B* ne dit rien.

20. *A* dit «Nous sommes tous les deux chevaliers» et *B* dit « *A* est un coquin. "

21. *A* dit «Je suis un chevalier ou *B* est un chevalier» et *B* ne dit rien.

22. Les deux *A* et *B* dire : « Je suis un chevalier. »

23. *A* dit «Nous sommes tous les deux des fripons» et *B* ne dit rien.

Les exercices 24 à 31 concernent les habitants d'une île sur laquelle il y a trois types de personnes: les chevaliers qui disent toujours la vérité, les fripons qui mentent toujours, et les espions (appelés normaux par Smullyan [Sm78]) qui peut mentir ou dire la vérité. Vous rencontrer trois personnes, *A* , *B* et *C* . Vous en connaissez un les gens sont un chevalier, l'un est un escroc et l'autre est un espion. Chacun de trois personnes connaissent le type de personne que chacune des deux autres est. Pour chacune de ces situations, si possible, détermine s'il y a est une solution unique et déterminer qui est le valet, le chevalier et espion sont. Lorsqu'il n'y a pas de solution unique, listez toutes les solutions possibles solutions ou déclarer qu'il n'y a pas de solutions.

24. *A* dit « *C* est le chevalier », *B* dit: « *A* est le chevalier» et *C* dit "Je suis l'espion".

25. *A* dit «Je suis le chevalier», *B* dit «Je suis le chevalier » et

Une branche mène aux ruines que vous souhaitez visiter; L'autre branche mène profondément dans la jungle. Un villageois est debout à la bifurcation de la route. Quelle question pouvez-vous poser au villageois pour déterminer quelle branche prendre?

16. Un explorateur est capturé par un groupe de cannibales. Il y a deux types de cannibales - ceux qui disent toujours la vérité et ceux qui mentent toujours. Les cannibales vont barbecue l'explorateur à moins qu'il ne puisse déterminer si un particulier cannibale ment toujours ou dit toujours la vérité. Il est autorisé à poser exactement une question aux cannibales.

a) Expliquez pourquoi la question «Êtes-vous un menteur?» ne travail.

b) Trouvez une question que l'explorateur peut utiliser pour déterminer si le cannibale ment toujours ou dit toujours au vérité.

17. Lorsque trois professeurs sont assis dans un restaurant, l'hôte ess leur demande: "Est-ce que tout le monde veut du café?" Le premier le professeur dit: "Je ne sais pas." Le deuxième professeur dit alors: "Je ne sais pas." Enfin, le troisième professeur dit: "Non, tout le monde ne veut pas de café." L'hôtesse vient retour et donne du café aux professeurs qui le veulent. Comment a-t-elle compris qui voulait du café?

18. Lorsque vous planifiez une fête, vous voulez savoir à qui vite. Parmi les personnes que vous souhaitez inviter, vous trouverez trois amis délicats. Vous savez que si Jasmine assiste, elle

C dit " B est le chevalier."

26. A dit «Je suis le valet», B dit «Je suis le valet» et C dit: "Je suis l'escroc".

27. A dit «Je suis le chevalier», B dit « A dit la vérité» et C dit "Je suis l'espion".

28. A dit «Je suis le chevalier», B dit: « A n'est pas le chevalier» , et C dit " B n'est pas le coquin".

29. A dit «Je suis le chevalier», B dit «Je suis le chevalier» et C dit: «Je suis le chevalier».

30. A dit «Je ne suis pas l'espion», B dit «Je ne suis pas l'espion» et C dit " A est l'espion."

31. A dit «Je ne suis pas l'espion», B dit «Je ne suis pas l'espion» et C dit: "Je ne suis pas l'espion."

Les exercices 32 à 38 sont des énigmes qui peuvent être résolues en traduisant déclarations en expressions logiques et raisonnement à partir de ces expressions utilisant des tables de vérité.

32. La police a trois suspects pour le meurtre de M. Cooper: M. Smith, M. Jones et M. Williams. Forgeron, Jones et Williams déclarent chacun qu'ils n'ont pas tué Tonnelier. Smith déclare également que Cooper était un ami de Jones et que Williams ne l'aimait pas. Jones déclare également qu'il ne connaissait pas Cooper et qu'il était hors de la ville le jour où Cooper a été tué. Williams déclare également qu'il

vu Smith et Jones avec Cooper le jour de la tuer et que Smith ou Jones doivent avoir tué lui. Pouvez-vous déterminer qui était le meurtrier si

a) l' un des trois hommes est coupable, les deux innocents disent la vérité, mais les déclarations des coupables l'homme peut ou peut ne pas être vrai?

b) les hommes innocents ne mentent pas?

33. Steve aimerait déterminer les salaires relatifs de trois collègues en utilisant deux faits. Tout d'abord, il sait que si Fred n'est pas la mieux payée des trois, alors Janice l'est. Seconde-Deuxièmement, il sait que si Janice n'est pas la moins bien payée, alors Maggie est la mieux payée. Est-il possible de déterminer salaires relatifs de Fred, Maggie et Janice de ce que Steve sait? Dans l'affirmative, qui est le plus payé et qui moins? Expliquez votre raisonnement.

34. Cinq amis ont accès à une salle de chat. est-ce possible de déterminer qui est en train de discuter si les informations suivantes sont connu? Kevin ou Heather, ou les deux, discutent. Randy ou Vijay, mais pas les deux, discutent. Si Abby parle, Randy aussi. Vijay et Kevin sont tous les deux le chat ou ni l'un ni l'autre. Si Heather discute, il en va de même Abby et Kevin. Expliquez votre raisonnement.

35. Un détective a interrogé quatre témoins d'un crime. D'après les histoires des témoins, le détective a conclu que si le majordome dit la vérité, il en est de même pour le cuisinier; le cuisinier et le jardinier ne peuvent pas tous les deux dire au vérité; le jardinier et le bricoleur ne mentent pas tous les deux; et si le bricoleur dit la vérité, alors le cuisinier est mensonge. Pour chacun des quatre témoins, le détective peut-il déterminer si cette personne dit la vérité ou ment? Expliquez votre raisonnement.

36. Quatre amis ont été identifiés comme suspects pour un abus accès théorisé à un système informatique. Ils ont fait déclarations aux autorités chargées de l'enquête. Dit Alice "Carlos l'a fait." John a dit "Je ne l'ai pas fait." Carlos a dit "Diana l'a fait." Diana a dit "Carlos a menti quand il a dit que Je l'ai fait."

a) Si les autorités savent également qu'exactement l'une des quatre suspects disent la vérité, qui l'a fait? Explique votre raisonnement.

b) Si les autorités savent également qu'une seule ment, qui l'a fait? Expliquez votre raisonnement.

37. Supposons qu'il y ait des panneaux sur les portes de deux pièces. le signe sur la première porte se lit "Dans cette pièce il y a une dame, et dans l'autre il y a un tigre »; et le signe sur le deuxième porte se lit "Dans l'une de ces chambres, il y a une dame, et dans l'un d'eux il y a un tigre. "Supposons que vous sachez que l'un de ces signes est vrai et que l'autre est faux.

dont la boisson préférée est l'eau minérale (qui est l'un des boissons préférées) étant donné ces indices: l'Anglais vit dans la maison rouge. L'Espagnol possède un chien. les Japonais l'homme est peintre. L'Italien boit du thé. Le norvégien vit dans la première maison à gauche. La maison verte est immédiatement à droite du blanc. La photographie pher élève des escargots. Le diplomate vit dans la maison jaune. Le lait se boit dans la maison du milieu. Le propriétaire du green maison boit du café. La maison du Norvégien est à côté de la le bleu. Le violoniste boit du jus d'orange. Le renard est en une maison à côté de celle du médecin. Le cheval est dans un maison à côté de celle du diplomate. [*Astuce:* faire un tableau où les lignes représentent les hommes et les colonnes représentent la couleur de leurs maisons, de leur travail, de leurs animaux de compagnie et boissons préférées et utiliser un raisonnement logique pour déterminer entrées correctes dans le tableau.]

39. La Freédonie compte cinquante sénateurs. Chaque sénateur est soit honnête ou corrompu. Supposons que vous sachiez qu'au moins un des sénateurs donian est honnête et que, étant donné deux Free-sénateurs donian, au moins un est corrompu. Sur la base de ces faits, pouvez-vous déterminer combien de sénateurs freedoniens sont honnêtes et combien sont corrompus? Si oui, quel est le répondre?

40. Trouvez la sortie de chacun de ces circuits combinatoires.

une) p

q

b) p

p

q

41. Trouvez la sortie de chacun de ces circuits combinatoires.

une) p

q

r

b) p

q

p

r

Derrière quelle porte se trouve la dame?

∗ **38.** Résolvez ce fameux puzzle logique attribué à Albert Ein- stein, et connu sous le nom de **puzzle de zèbre** . Cinq hommes avec différentes nationalités et avec des emplois différents vivent en maisons isolées dans une rue. Ces maisons sont peintes différentes couleurs. Les hommes ont différents animaux de compagnie et différentes boissons préférées. Déterminez à qui appartient un zèbre et

42. Construire un circuit combinatoire utilisant des onduleurs, Portes OU et portes ET qui produisent la sortie $(p \wedge \neg r) \vee (\neg q \wedge r)$ à partir des bits d'entrée p , q et r .

43. Construire un circuit combinatoire utilisant des onduleurs, Portes OU et portes ET qui produisent la sortie $((\neg p \vee \neg r) \wedge \neg q) \vee (\neg p \wedge (q \vee r))$ à partir des bits d'entrée p , q et r .

Équivalences propositionnelles

introduction

Un type important d'étape utilisé dans un argument mathématique est le remplacement d'une instruction avec une autre déclaration avec la même valeur de vérité. Pour cette raison, les méthodes qui produisent Les positions ayant la même valeur de vérité qu'une proposition composée donnée sont largement utilisées construction d'arguments mathématiques. Notez que nous utiliserons le terme «proposition »pour désigner une expression formée de variables propositionnelles utilisant des opérateurs logiques, comme $p \wedge q$.

Nous commençons notre discussion par une classification des propositions composées selon leur valeurs de vérité possibles.

DÉFINITION 1 Une proposition composée qui est toujours vraie, quelles que soient les valeurs de vérité de la proposition. Les variables supplémentaires qui s'y produisent sont appelées *tautologie* . Une proposition composée toujours faux est appelé une *contradiction* . Une proposition composée qui n'est ni une tautologie ni un la contradiction est appelée *contingence* .

Les tautologies et les contradictions sont souvent importantes dans le raisonnement mathématique. Exemple 1 illus- traite ces types de propositions composées.

EXEMPLE 1 Nous pouvons construire des exemples de tautologies et de contradictions en utilisant une seule variation propositionnelle. capable. Considérons les tables de vérité de $p \vee \neg p$ et $p \wedge \neg p$, présentées dans le tableau 1. Parce que $p \vee \neg p$ est toujours vrai, c'est une tautologie. Parce que $p \wedge \neg p$ est toujours faux, c'est une contradiction. ▲

Équivalences logiques

Les propositions composées qui ont les mêmes valeurs de vérité dans tous les cas possibles sont appelées **logiquement équivalent** . Nous pouvons également définir cette notion comme suit.

DÉFINITION 2 Les propositions composées p et q sont dites *logiquement équivalentes* si $p \leftrightarrow q$ est une tautologie. La notation $p \equiv q$ indique que p et q sont logiquement équivalents.

Remarque: Le symbole ≡ n'est pas un connecteur logique, et $p \equiv q$ n'est pas une proposition composée mais plutôt l'affirmation que $p \leftrightarrow q$ est une tautologie. Le symbole ⇔ est parfois utilisé à la place de ≡ pour désigner l'équivalence logique.

Une façon de déterminer si deux propositions composées sont équivalentes consiste à utiliser une vérité table. En particulier, les propositions composées p et q sont équivalentes si et seulement si les colonnes

TABLEAU 1 Exemples de tautologie et une contradiction.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

TABLEAU 2 De
Les lois de Morgan.

$\neg(p \wedge q) \equiv \neg p \vee \neg q$

$\neg(p \vee q) \equiv \neg p \wedge \neg q$

donner leurs valeurs de vérité d'accord. L'exemple 2 illustre cette méthode pour établir un équivalence logique importante et utile, à savoir celle de $\neg(p \vee q)$ avec $\neg p \wedge \neg q$. Cette logique l'équivalence est l'une des deux **lois De Morgan** , présentées dans le tableau 2, du nom de l'anglais mathématicien Augustus De Morgan, du milieu du XIXe siècle.

EXEMPLE 2 Montrer que $\neg(p \vee q)$ et $\neg p \wedge \neg q$ sont logiquement équivalents.

Solution: les tables de vérité pour ces propositions composées sont affichées dans le tableau 3. Parce que les valeurs de vérité des propositions composées $\neg(p \vee q)$ et $\neg p \wedge \neg q$ s'accordent pour tous les possibles combinaisons des valeurs de vérité de p et q , il s'ensuit que $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ est une tautologie et que ces propositions composées sont logiquement équivalentes. ▲

TABLEAU 3 Tables de vérité pour $\neg(p \vee q)$ et $\neg p \wedge \neg q$.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

EXEMPLE 3 Montrer que $p \rightarrow q$ et $\neg p \vee q$ sont logiquement équivalents.

Solution: Nous construisons la table de vérité pour ces propositions composées dans le tableau 4. Parce que le les valeurs de vérité de $\neg p \vee q$ et $p \rightarrow q$ concordent, elles sont logiquement équivalentes. ▲

TABLEAU 4 Tables de vérité pour $\neg p \vee q$ et $p \rightarrow q$.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Nous allons maintenant établir une équivalence logique de deux propositions composées impliquant trois différentes variables propositionnelles p , q et r . Pour utiliser une table de vérité pour établir une telle logique équivalence, nous avons besoin de huit lignes, une pour chaque combinaison possible de valeurs de vérité de ces trois variables. Nous représentons symboliquement ces combinaisons en listant les valeurs de vérité de p , q et r , respectivement. Ces huit combinaisons de valeurs de vérité sont TTT, TTF, TFT, TFF, FTT, FTF, FFT et FFF; nous utilisons cet ordre lorsque nous affichons les lignes de la table de vérité. Notez que nous besoin de doubler le nombre de lignes dans les tables de vérité que nous utilisons pour montrer que les propositions composées sont équivalentes pour chaque variable propositionnelle supplémentaire, de sorte que 16 lignes sont nécessaires pour établir l'équivalence logique de deux propositions composées impliquant quatre variables propositionnelles, etc. En général, 2^n des lignes sont requises si une proposition composée implique n propositionnelle variables.

TABLEAU 5 **Démonstration que $p \lor (q \land r)$ et $(p \lor q) \land (p \lor r)$ sont logiquement Équivalent.**

p	q	r	$q \land r$	$p \lor (q \land r)$	$p \lor q$	$p \lor r$	$(p \lor q) \land (p \lor r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

EXEMPLE 4 Montrer que $p \lor (q \land r)$ et $(p \lor q) \land (p \lor r)$ sont logiquement équivalents. C'est le *distributif loi* de disjonction sur la conjonction.

Solution: Nous construisons la table de vérité pour ces propositions composées dans le tableau 5. Parce que les valeurs de vérité de $p \lor (q \land r)$ et $(p \lor q) \land (p \lor r)$ concordent, ces propositions composées sont logiquement équivalent. ▲

Les identités du tableau 6 sont un cas particulier de Identités d'algèbre booléenne trouvé dans le tableau 5 de Section 12.1. Voir tableau 1 dans la section 2.2 pour identités de jeu analogues.

Le tableau 6 contient quelques équivalences importantes. Dans ces équivalences, **T** désigne la com- proposition de livre qui est toujours vraie et **F** désigne la proposition composée qui est toujours

TABLEAU 6 **Équivalences logiques.**

Équivalence	*Nom*
$p \land \mathbf{T} \equiv p$ $p \lor \mathbf{F} \equiv p$	Lois sur l'identité
$p \lor \mathbf{T} \equiv \mathbf{T}$ $p \land \mathbf{F} \equiv \mathbf{F}$	Lois de domination
$p \lor p \equiv p$ $p \land p \equiv p$	Lois idempotentes
$\neg(\neg p) \equiv p$	Loi de double négation
$p \lor q \equiv q \lor p$ $p \land q \equiv q \land p$	Lois commutatives
$(p \lor q) \lor r \equiv p \lor (q \lor r)$ $(p \land q) \land r \equiv p \land (q \land r)$	Lois associatives
$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$ $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$	Lois distributives
$\neg(p \land q) \equiv \neg p \lor \neg q$ $\neg(p \lor q) \equiv \neg p \land \neg q$	Les lois de De Morgan
$p \lor (p \land q) \equiv p$ $p \land (p \lor q) \equiv p$	Lois d'absorption
$p \lor \neg p \equiv \mathbf{T}$ $p \land \neg p \equiv \mathbf{F}$	Lois de négation

TABLEAU 7 **Équivalences logiques Impliquer des instructions conditionnelles.**

$p \to q \equiv \neg p \lor q$
$p \to q \equiv \neg q \to \neg p$
$p \lor q \equiv \neg p \to q$
$p \land q \equiv \neg (p \to \neg q)$
$\neg (p \to q) \equiv p \land \neg q$
$(p \to q) \land (p \to r) \equiv p \to (q \land r)$
$(p \to r) \land (q \to r) \equiv (p \lor q) \to r$
$(p \to q) \lor (p \to r) \equiv p \to (q \lor r)$
$(p \to r) \lor (q \to r) \equiv (p \land q) \to r$

TABLEAU 8 **Logique Équivalences impliquant Déclarations biconditionnelles.**

$p \leftrightarrow q \equiv (p \to q) \land (q \to p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$
$\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

faux. Nous montrons également quelques équivalences utiles pour les propositions composées impliquant les déclarations conditionnelles et les déclarations biconditionnelles des tableaux 7 et 8, respectivement.Le lecteur est demandé de vérifier les équivalences dans les tableaux 6 à 8 des exercices.

La loi associative de disjonction montre que l'expression $p \lor q \lor r$ est bien définie, dans le sens où il importe peu que l'on prenne d'abord la disjonction de p avec q puis la disjonction de $p \lor q$ avec r , ou si nous prenons d'abord la disjonction de q et r , puis prenons la disjonction de p avec $q \lor r$. De même, l'expression $p \land q \land r$ est bien définie. En étendant ce raisonnement, il s'ensuit que $p_1 \lor p_2 \lor \cdots \lor p_n$ et $p_1 \land p_2 \land \cdots \land p_n$ sont bien définis chaque fois $p_1, p_2, \ldots, p_n$ sont des propositions.

En outre, notez que les lois de De Morgan s'étendent aux

$$\neg (p_1 \lor p_2 \lor \cdots \lor p_n) \equiv (\neg p_1 \land \neg p_2 \land \cdots \land \neg p_n)$$

et

$$\neg (p_1 \land p_2 \land \cdots \land p_n) \equiv (\neg p_1 \lor \neg p_2 \lor \cdots \lor \neg p_n).$$

Nous utiliserons parfois la notation $\bigvee_{j=1}^{n} p_j$ pour $p_1 \lor p_2 \lor \cdots \lor p_n$ et $\bigwedge_{j=1}^{n} p_j$ pour $p_1 \land p_2 \land \cdots \land p_n$. En utilisant cette notation, la version étendue des lois de De Morgan peut être écrit avec concision comme $\neg \left(\bigvee_{j=1}^{n} p_j\right) \equiv \bigwedge_{j=1}^{n} \neg p_j$ et $\neg \left(\bigwedge_{j=1}^{n} p_j\right) \equiv \bigvee_{j=1}^{n} \neg p_j$. (Méthodes pour la preuve de ces identités sera donnée dans la section 5.1.)

Utilisation des lois de De Morgan

Lors de l'utilisation de De Morgan's lois, pensez à changer le connecteur logique après avoir nié.

Les deux équivalences logiques connues sous le nom de lois de De Morgan sont particulièrement importantes.Ils disent nous comment nier les conjonctions et comment nier les disjonctions.En particulier, l'équivalence $\neg (p \lor q) \equiv \neg p \land \neg q$ nous dit que la négation d'une disjonction se forme en prenant la conjonction des négations des propositions composantes. De même, l'équivalence $\neg (p \land q) \equiv \neg p \lor \neg q$ nous dit que la négation d'une conjonction se forme en prenant la disjonction de la négations des propositions de composants. L'exemple 5 illustre l'utilisation des lois de De Morgan.

EXEMPLE 5 Utilisez les lois de De Morgan pour exprimer les négations de «Miguel a un téléphone portable et il a un ordinateur portable ordinateur "et" Heather ira au concert ou Steve ira au concert. "

Solution: Soit p «Miguel a un téléphone portable» et q soit «Miguel a un ordinateur portable». Ensuite «Miguel a un téléphone portable et un ordinateur portable» peut être représenté par $p \wedge q$. Par le première des lois de De Morgan, $\neg(p \wedge q)$ équivaut à $\neg p \vee \neg q$. Par conséquent, nous pouvons exprimer la négation de notre déclaration d'origine comme «Miguel n'a pas de téléphone portable ou il n'a pas un ordinateur portable. "

Soit r «Heather ira au concert» et s «Steve ira au concert». Ensuite «Heather ira au concert ou Steve ira au concert» peut être représenté par $r \vee s$. Par la seconde des lois de De Morgan, $\neg(r \vee s)$ équivaut à $\neg r \wedge \neg s$. Par conséquent, nous pouvons exprimer la négation de notre déclaration originale comme «Heather n'ira pas au concert et Steve n'ira pas au concert. " ▲

Construire de nouvelles équivalences logiques

Les équivalences logiques du tableau 6, ainsi que toutes les autres qui ont été établies (telles que ceux indiqués dans les tableaux 7 et 8), peuvent être utilisés pour construire des équivalences logiques supplémentaires.le la raison en est qu'une proposition dans une proposition composée peut être remplacée par un composé proposition qui lui est logiquement équivalente sans changer la valeur de vérité de l'original proposition composée. Cette technique est illustrée dans les exemples 6 à 8, où nous utilisons également fait que si p et q sont logiquement équivalents et q et r sont logiquement équivalents, alors p et r sont logiquement équivalents (voir exercice 56).

EXEMPLE 6 Montrer que $\neg(p \to q)$ et $p \wedge \neg q$ sont logiquement équivalents.

Solution: nous pourrions utiliser une table de vérité pour montrer que ces propositions composées sont équivalentes (similaire à ce que nous avons fait dans l'exemple 4). En effet, il ne serait pas difficile de le faire.Cependant, nous voulons pour illustrer comment utiliser les identités logiques que nous connaissons déjà pour établir de nouvelles identités logiques, quelque chose qui est d'une importance pratique pour établir des équivalences de propositions composées avec un grand nombre de variables. Nous allons donc établir cette équivalence en développant une série de

AUGUSTUS DE MORGAN (1806–1871) Augustus De Morgan est né en Inde, où son père était colonel dans l'armée indienne. La famille de De Morgan a déménagé en Angleterre à l'âge de 7 mois. Il a assisté les écoles privées où, au début de son adolescence, il a développé un vif intérêt pour les mathématiques. De Morgan a étudié au Trinity College, Cambridge, diplômé en 1827. Bien qu'il envisageait la médecine ou le droit, il décida mathématiques pour sa carrière. Il a obtenu un poste à l'University College de Londres en 1828, mais a démissionné après la l'université a renvoyé un collègue professeur sans donner de raisons. Cependant, il reprend ce poste en 1836 lorsque son successeur est décédé, restant jusqu'en 1866.

De Morgan était un enseignant réputé qui insistait sur les principes plutôt que sur les techniques. Ses étudiants comprenaient de nombreux célèbres mathématiciens, dont Augusta Ada, comtesse de Lovelace, qui était le collaborateur de Charles Babbage dans son travaux sur des machines informatiques (voir page 31 pour les notes biographiques sur Augusta Ada). (De Morgan a mis en garde la comtesse contre étudier trop de mathématiques, car cela pourrait interférer avec ses capacités de procréation!)

De Morgan était un écrivain extrêmement prolifique, publiant plus de 1000 articles dans plus de 15 périodiques. De Morgan aussi a écrit des manuels sur de nombreux sujets, y compris la logique, la probabilité, le calcul et l'algèbre. En 1838, il a présenté ce qui était peut-être le premier explication claire d'une technique de preuve importante connue sous le nom d' *induction mathématique* (discutée dans la section 5.1 de ce texte), un terme il a inventé. Dans les années 1840, De Morgan a apporté des contributions fondamentales au développement de la logique symbolique. Il a inventé les notations cela l'a aidé à prouver les équivalences propositionnelles, telles que les lois qui portent son nom. En 1842, De Morgan a présenté ce est considérée comme la première définition précise d'une limite et a développé de nouveaux tests de convergence de séries infinies. De Morgan était s'intéresse également à l'histoire des mathématiques et écrit des biographies de Newton et Halley.

En 1837, De Morgan a épousé Sophia Frend, qui a écrit sa biographie en 1882. La recherche, l'écriture et l'enseignement de De Morgan sont partis peu de temps pour sa vie familiale ou sociale. Néanmoins, il était reconnu pour sa gentillesse, son humour et son large éventail de connaissances.

équivalences logiques, en utilisant l'une des équivalences du tableau 6 à la fois, en commençant par $\neg(p \to q)$ et se terminant par $p \wedge \neg q$. Nous avons les équivalences suivantes.

$$\begin{aligned} \neg(p \to q) &\equiv \neg(\neg p \vee q) && \text{par l'exemple 3} \\ &\equiv \neg(\neg p) \wedge \neg q && \text{par la deuxième loi De Morgan} \\ &\equiv p \wedge \neg q && \text{par la loi de la double négation} \end{aligned}$$

▲

EXEMPLE 7 Montrer que $\neg(p \vee (\neg p \wedge q))$ et $\neg p \wedge \neg q$ sont logiquement équivalents en développant une série de équivalences logiques.

Solution: Nous allons utiliser l'une des équivalences du tableau 6 à la fois, en commençant par $\neg(p \vee (\neg p \wedge q))$ et se terminant par $\neg p \wedge \neg q$. (*Remarque:* nous pourrions également facilement établir cette équivalence en utilisant une vérité tableau.) Nous avons les équivalences suivantes.

$$\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg(\neg p \wedge q) \quad \text{par la deuxième loi De Morgan}$$
$$\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] \quad \text{par la première loi De Morgan}$$
$$\equiv \neg p \wedge (p \vee \neg q) \quad \text{par la loi de la double négation}$$
$$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \quad \text{par la deuxième loi distributive}$$
$$\equiv \mathbf{F} \vee (\neg p \wedge \neg q) \quad \text{parce que } \neg p \wedge p \equiv \mathbf{F}$$
$$\equiv (\neg p \wedge \neg q) \vee \mathbf{F} \quad \text{par la loi commutative de disjonction}$$
$$\equiv \neg p \wedge \neg q \quad \text{par la loi sur l'identité pour } \mathbf{F}$$

Par conséquent $\neg(p \vee (\neg p \wedge q))$ et $\neg p \wedge \neg q$ sont logiquement équivalents. ▲

EXEMPLE 8 Montrer que $(p \wedge q) \rightarrow (p \vee q)$ est une tautologie.

Solution: Pour montrer que cette affirmation est une tautologie, nous utiliserons des équivalences logiques pour Strate qu'il est logiquement équivalent à **T** . (*Remarque:* cela pourrait également être fait à l'aide d'une table de vérité.)

$$(p \wedge q) \rightarrow (p \vee q) \equiv \neg(p \wedge q) \vee (p \vee q) \quad \text{par l'exemple 3}$$
$$\equiv (\neg p \vee \neg q) \vee (p \vee q) \quad \text{par la première loi De Morgan}$$
$$\equiv (\neg p \vee p) \vee (\neg q \vee q) \quad \text{par l'associatif et le commutatif lois de disjonction}$$
$$\equiv \mathbf{T} \vee \mathbf{T} \quad \text{par l'exemple 1 et le commutatif loi de disjonction}$$
$$\equiv \mathbf{T} \quad \text{par la loi de domination}$$

▲

Satisfaction propositionnelle

Une proposition composée est **satisfaisable** s'il existe une affectation de valeurs de vérité à ses variables qui rend cela vrai. En l'absence de telles affectations, c'est-à-dire lorsque la proposition composée est fausse pour toutes les affectations de valeurs de vérité à ses variables, la proposition composée n'est **pas satisfaisante** . Notez qu'une proposition composée n'est pas satisfaisante si et seulement si sa négation est vraie pour tous affectations de valeurs de vérité aux variables, c'est-à-dire si et seulement si sa négation est une tautologie.

Lorsque nous trouvons une affectation particulière de valeurs de vérité qui fait une proposition composée c'est vrai, nous avons montré qu'il est satisfaisable; une telle affectation est appelée une **solution** de ce particulier

problème de satisfiabilité. Cependant, pour montrer qu'une proposition composée n'est pas satisfaisante, nous devons pour montrer que *chaque* affectation de valeurs de vérité à ses variables la rend fausse. Bien que nous puissions utilisez toujours une table de vérité pour déterminer si une proposition composée est satisfaisable, il est souvent plus efficace de ne pas le faire, comme le montre l'exemple 9.

EXEMPLE 9 Déterminer si chacune des propositions composées $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$, et $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ est satisfaisable.

Solution: Au lieu d'utiliser la table de vérité pour résoudre ce problème, nous raisonnerons sur les valeurs de vérité. Notez que $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ est vrai lorsque les trois variables p , q et r ont la même valeur de vérité (voir l'exercice 40 de la section 1.1).Par conséquent, il est satisfaisant car il y a au moins une affectation de valeurs de vérité pour p , q et r qui la rend vraie. De même, notez que $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ est vrai quand au moins l'un de p , q et r est vrai et au moins un est faux (voir l'exercice 41 de la section 1.1).Donc, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ est satisfiable, car il y a au moins une affectation de valeurs de vérité pour p , q et r qui la rend vraie.

Enfin, notez que pour $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ pour être vrai, $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$ et $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ doivent tous deux Sois sincère. Pour que la première soit vraie, les trois variables doivent avoir les mêmes valeurs de vérité, et pour que la seconde soit vraie, au moins une des trois variables doit être vraie et au moins une doit être faux. Cependant, ces conditions sont contradictoires. De ces observations, nous concluons qu'aucune affectation de valeurs de vérité à p , q et r *ne* fait $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ vrai. Par conséquent, il n'est pas satisfaisant. ▲

AUGUSTA ADA, COMTESSE DE LOVELACE (1815–1852) Augusta Ada était la seule enfant de la mariage du célèbre poète Lord Byron et Lady Byron, Annabella Millbanke, qui se sont séparés quand Ada avait 1 mois, en raison de la scandaleuse liaison de Lord Byron avec sa demi-sœur. Le Lord Byron avait tout un réputation, décrite par l'un de ses amants comme «folle, mauvaise et dangereuse à connaître». Lady Byron était connue pour son intellect et avait une passion pour les mathématiques; elle a été appelée par Lord Byron «La princesse des parallélogrammes». Augusta a été élevée par sa mère, qui a encouragé ses talents intellectuels en particulier en musique et en mathématiques, pour contrer ce que Lady Byron considérait comme des tendances poétiques dangereuses. A cette époque, les femmes n'étaient pas autorisées à fréquenter les universités et ne pouvait pas rejoindre les sociétés savantes. Néanmoins, Augusta a poursuivi ses études mathématiques indépendamment et avec des mathématiciens, dont William Frend. Elle a également été encouragée par une autre femme mathématicienne, Mary Somerville, et en 1834 lors d'un dîner organisé par Mary Somerville, elle apprit l'histoire de Charles Babbage des idées pour une machine à calculer, appelée le moteur analytique. En 1838, Augusta Ada épousa Lord King, plus tard élevé au comte de Lovelace. Ensemble, ils ont eu trois enfants.

Augusta Ada a poursuivi ses études de mathématiques après son mariage. Charles Babbage avait poursuivi ses travaux sur son analyse Moteur et donné des conférences à ce sujet en Europe. En 1842, Babbage demanda à Augusta Ada de traduire un article en français décrivant la invention. Lorsque Babbage a vu sa traduction, il lui a suggéré d'ajouter ses propres notes, et le travail résultant a été trois fois longueur de l'original. Les comptes rendus les plus complets du moteur analytique se trouvent dans les notes d'Augusta Ada. Dans ses notes, elle a comparé le fonctionnement du moteur analytique à celui du métier Jacquard, avec les cartes perforées de Babbage analogues aux cartes utilisées pour créer des motifs sur le métier. En outre, elle a reconnu la promesse de la machine comme un ordinateur à usage général beaucoup mieux que Babbage. Elle a déclaré que le «moteur est l'expression matérielle de toute fonction indéfinie de tout degré de généralité et complexité. »Ses notes sur le moteur analytique anticipent de nombreux développements futurs, y compris la musique générée par ordinateur. Augusta Ada a publié ses écrits sous ses initiales AAL dissimulant son identité de femme comme beaucoup de femmes à une époque où les femmes n'étaient pas considérés comme les égaux intellectuels des hommes. Après 1845, elle et Babbage ont travaillé au développement d'un système pour prédire les courses de chevaux. Malheureusement, leur système n'a pas bien fonctionné, laissant Augusta Ada lourdement endettée au moment de sa mort à un âge malheureusement jeune du cancer de l'utérus.

En 1953, les notes d'Augusta Ada sur le moteur analytique ont été republiées plus de 100 ans après leur rédaction et après ils avaient été oubliés depuis longtemps. Dans son travail des années 50 sur la capacité des ordinateurs à penser (et son fameux test de Turing), Alan Turing a répondu à la déclaration d'Augusta Ada selon laquelle «le moteur analytique n'a aucune prétention à l'origine de quoi que ce soit. Ça peut faire quoi que nous sachions comment lui ordonner de se produire. »Ce« dialogue »entre Turing et Augusta Ada fait toujours l'objet de controverses. En raison de ses contributions fondamentales à l'informatique, le langage de programmation Ada est nommé en l'honneur de la comtesse de Lovelace.

2 9 4
5 1
4
4 2
6 sept
5
sept 3 5
1 9
6

FIGURE 1 Un puzzle Sudoku 9 × 9.

Applications de la satisfaction

De nombreux problèmes, dans divers domaines tels que la robotique, les tests de logiciels, la conception assistée par ordinateur, la vision industrielle, la conception de circuits intégrés, les réseaux informatiques et la génétique peuvent être modélisés en termes de satisfiabilité propositionnelle. Bien que la plupart de ces applications dépassent portée de ce livre, nous étudierons une application ici. En particulier, nous montrerons comment utiliser Satisfaction propositionnelle pour modéliser des puzzles Sudoku.

SUDOKU Un **puzzle Sudoku** est représenté par une grille 9 × 9 composée de neuf sous-grilles 3 × 3, appelés **blocs** , comme le montre la figure 1. Pour chaque puzzle, certaines des 81 cellules, appelées **givens** , se voient attribuer l'un des numéros 1 , 2 , ..., 9 et les autres cellules sont vides. Le puzzle est résolu en attribuant un numéro à chaque cellule vide de sorte que chaque ligne, chaque colonne et chacune des neuf blocs 3 × 3 contiennent chacun des neuf nombres possibles. Notez qu'au lieu d'utiliser un 9 × 9 grille, les puzzles Sudoku peuvent être basés sur $n^2 \times n^2$ grilles, pour tout entier positif n , avec les $n^2 \times n^2$ grille composée de n^2 $n \times n$ *sous-* grilles.

La popularité du Sudoku remonte aux années 1980 quand il a été introduit au Japon. Il Il a fallu 20 ans pour que le Sudoku se propage au reste du monde, mais en 2005, les puzzles Sudoku étaient un engouement mondial. Le nom Sudoku est l'abréviation du japonais *suuji wa dokushin ni kagiru* , qui signifie "les chiffres doivent rester simples". Le jeu moderne de Sudoku a apparemment été conçu à la fin des années 1970 par un concepteur de puzzle américain. Les idées de base du Sudoku remontent même plus loin; les puzzles imprimés dans les journaux français dans les années 1890 étaient assez similaires, mais pas identiques, au Sudoku moderne.

Les puzzles Sudoku conçus pour le divertissement ont deux propriétés importantes supplémentaires. Premier, ils ont exactement une solution. Deuxièmement, ils peuvent être résolus en utilisant le raisonnement seul, c'est-à-dire sans recourir à la recherche de toutes les attributions possibles de numéros aux cellules. Comme un puzzle Sudoku est résolus, les entrées dans les cellules vides sont successivement déterminées par des valeurs déjà connues. Par exemple, dans la grille de la figure 1, le chiffre 4 doit apparaître dans exactement une cellule de la deuxième ligne. Comment pouvons-nous déterminer laquelle des sept cellules vierges il doit apparaître? Tout d'abord, nous observons que 4 ne peuvent pas apparaissent dans l'une des trois premières cellules ou dans l'une des trois dernières cellules de cette ligne, car apparaît dans une autre cellule du bloc où se trouve chacune de ces cellules. On peut aussi voir que 4 ne peuvent pas apparaître dans la cinquième cellule de cette ligne, comme cela apparaît déjà dans la cinquième colonne de la quatrième ligne. Ça signifie que 4 doit apparaître dans la sixième cellule de la deuxième ligne.

De nombreuses stratégies basées sur la logique et les mathématiques ont été conçues pour résoudre le Sudoku des puzzles (voir [Da10], par exemple). Ici, nous discutons l'une des façons qui ont été développées pour résoudre des puzzles Sudoku à l'aide d'un ordinateur, ce qui dépend de la modélisation du puzzle comme un problème de satisfiabilité propositionnelle. En utilisant le modèle que nous décrivons, des puzzles Sudoku particuliers peut être résolu en utilisant un logiciel développé pour résoudre des problèmes de satisfiabilité. Actuellement, Sudoku les puzzles peuvent être résolus en moins de 10 millisecondes de cette façon. Il convient de noter qu'il existe de nombreuses autres approches pour résoudre des puzzles de Sudoku via des ordinateurs utilisant d'autres techniques.

Pour encoder un puzzle Sudoku, notons $p(i, j, n)$ la proposition qui est vraie lorsque le nombre n est dans la cellule de la i ème ligne et de la j ème colonne. Il y a 9 × 9 × 9 = 729 de telles propositions, comme i, j et n vont tous de 1 à 9. Par exemple, pour le casse-tête de la figure 1, le nombre 6 est donné comme valeur dans la cinquième ligne et la première colonne. Par conséquent, nous voyons que $p(5, 1, 6)$ est vrai, mais $p(5, j, 6)$ est faux pour $j = 2, 3, \ldots, 9$.

Étant donné un puzzle Sudoku particulier, nous commençons par encoder chacune des valeurs données. Alors, nous construisons des propositions composées qui affirment que chaque ligne contient chaque nombre, chaque la colonne contient chaque numéro, chaque bloc 3 × 3 contient chaque numéro et chaque cellule contient pas plus d'un numéro. Il s'ensuit, comme le lecteur doit vérifier, que le puzzle Sudoku est résolu en trouvant une affectation de valeurs de vérité aux 729 propositions $p(i, j, n)$ avec i, j et n chacune allant de 1 à 9, ce qui rend la conjonction de toutes ces propositions composées vraie. Après En énumérant ces assertions, nous expliquerons comment construire l'assertion selon laquelle chaque ligne contient chaque entier de 1 à 9. Nous laisserons la construction des autres affirmations que chaque colonne contient chaque numéro et chacun des neuf blocs 3 × 3 contient chaque numéro des exercices.

- Pour chaque cellule avec une valeur donnée, nous affirmons $p(i, j, n)$ lorsque la cellule de la ligne i et de la colonne j a la valeur donnée n.
- Nous affirmons que chaque ligne contient chaque numéro:

$$\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$$

- Nous affirmons que chaque colonne contient chaque numéro:

$$\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i, j, n)$$

- Nous affirmons que chacun des neuf blocs 3 × 3 contient chaque nombre:

Il est difficile de configurer deux indices internes de sorte que les neuf cellules de chacune bloc carré sont examiné.

$$\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r+i, 3s+j, n)$$

- Pour affirmer qu'aucune cellule ne contient plus d'un nombre, nous prenons la conjonction sur tous valeurs de n, n, i et j où chaque variable varie de 1 à 9 et $n = n$ de $p(i, j, n) \rightarrow \neg p(i, j, n)$.

Nous expliquons maintenant comment construire l'assertion selon laquelle chaque ligne contient chaque nombre. Tout d'abord, pour affirmer que la ligne i contient le nombre n, nous formons $\bigvee_{j=1}^{9} p(i, j, n)$. Pour affirmer que la ligne i contient tous les n nombres, nous formons la conjonction de ces disjonctions sur les neuf valeurs possibles de n, nous donnant $\bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$. Enfin, pour affirmer que chaque ligne contient chaque nombre, nous prenons la conjonction de $\bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$ sur les neuf rangées. Cela donne nous $\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i, j, n)$. (Les exercices 65 et 66 demandent des explications sur les affirmations chaque colonne contient chaque numéro et que chacun des neuf blocs 3 × 3 contient chaque nombre.)

Étant donné un puzzle Sudoku particulier, pour résoudre ce puzzle, nous pouvons trouver une solution à la problèmes de bilité qui demandent un ensemble de valeurs de vérité pour les 729 variables $p(i, j, n)$ qui rend le conjonction de toutes les affirmations énumérées vrai.

Résolution des problèmes de satisfaction

Une table de vérité peut être utilisée pour déterminer si une proposition composée est satisfaisable ou par conséquent, si sa négation est une tautologie (voir exercice 60). Cela peut être fait à la main pour une proposition composée avec un petit nombre de variables, mais lorsque le nombre de variables grandit, cela devient peu pratique. Par exemple, il y a $2^{20} = 1,048,576$ lignes dans la vérité ble pour une proposition composée de 20 variables. De toute évidence, vous avez besoin d'un ordinateur pour vous aider déterminer, de cette manière, si une proposition composée à 20 variables est satisfaisable.

Lorsque de nombreuses applications sont modélisées, des questions concernant la satisfiabilité du composé des propositions avec des centaines, des milliers ou des millions de variables apparaissent. Notez, par exemple, que quand il y a 1000 variables, vérifier chacune des 2^{1000} (un nombre avec plus de 300 chiffres décimaux) combinaisons possibles de valeurs de vérité des variables dans une proposition composée ne peut pas être fait par un ordinateur, même en milliards d'années. Aucune procédure n'est connue ordinateur peut suivre pour déterminer dans un délai raisonnable si un composé arbitraire proposition dans un si grand nombre de variables est satisfaisable. Cependant, des progrès ont été réalisés développer des méthodes pour résoudre le problème de satisfiabilité pour des types particuliers de composés propositions qui se posent dans des applications pratiques, comme pour la solution de puzzles Sudoku. De nombreux programmes informatiques ont été développés pour résoudre des problèmes de satisfiabilité utilisation pratique. Dans notre discussion du sujet des algorithmes au chapitre 3, nous discuterons de cette question plus loin. En particulier, nous expliquerons le rôle important de la satisfiabilité propositionnelle jeux de problèmes dans l'étude de la complexité des algorithmes.

Des exercices

1. Utilisez des tables de vérité pour vérifier ces équivalences.

a) $p \wedge \mathbf{T} \equiv p$ **b)** $p \vee \mathbf{F} \equiv p$
c) $p \wedge \mathbf{F} \equiv \mathbf{F}$ **d)** $p \vee \mathbf{T} \equiv \mathbf{T}$
e) $p \vee p \equiv p$ **f)** $p \wedge p \equiv p$

2. Montrez que $\neg(\neg p)$ et p sont logiquement équivalents.

3. Utilisez des tables de vérité pour vérifier les lois commutatives

a) $p \vee q \equiv q \vee p$. **b)** $p \wedge q \equiv q \wedge p$.

4. Utilisez des tables de vérité pour vérifier les lois associatives

a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$.

b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

5. Utilisez une table de vérité pour vérifier la loi distributive $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.

6. Utilisez une table de vérité pour vérifier la première loi De Morgan $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

7. Utilisez les lois de De Morgan pour trouver la négation de chacun des les déclarations suivantes.

a) Jan est riche et heureux.

b) Carlos fera du vélo ou courra demain.

HENRY MAURICE SHEFFER (1883–1964) Henry Maurice Sheffer, né de parents juifs dans l'ouest du pays L'Ukraine a émigré aux États-Unis en 1892 avec ses parents et six frères et sœurs. Il a étudié au Boston Latin Avant d'entrer à Harvard, où il a obtenu son diplôme de premier cycle en 1905, sa maîtrise en 1907, et son doctorat. en philosophie en 1908. Après avoir occupé un poste postdoctoral à Harvard, Henry s'est rendu en Europe sur une bourse. À son retour aux États-Unis, il est devenu un nomade universitaire, passant un an chacun à l'Université de Washington, Cornell, l'Université du Minnesota, l'Université du Missouri et City Collège à New York. En 1916, il revient à Harvard en tant que membre du corps professoral du département de philosophie. Il est resté à Harvard jusqu'à sa retraite en 1952.

Sheffer a introduit ce qui est maintenant connu comme le coup de Sheffer en 1913; il n'est devenu connu qu'après son utilisation dans l'édition de 1925 de Whitehead et Russell's *Principia Mathematica* . Dans cette même édition, Russell a écrit que Sheffer avait inventé une méthode puissante qui pourrait être utilisée pour simplifier les *Principia* . À cause de ce commentaire, Sheffer était un homme mystérieux aux logiciens, surtout parce que Sheffer, qui a peu publié dans sa carrière, n'a jamais publié les détails de cette méthode, décrivant seulement dans des notes polycopiées et dans un bref résumé publié.

Sheffer était un professeur dévoué de logique mathématique. Il aimait que ses cours soient petits et n'aimait pas les auditeurs. Quand des étrangers apparu dans sa classe, Sheffer leur ordonnerait de partir, même ses collègues ou distingués invités visitant Harvard. Sheffer mesurait à peine cinq pieds; il était réputé pour son esprit et sa vigueur, ainsi que pour sa nervosité et son irritabilité. Bien que très apprécié, il était assez solitaire. Il est connu pour une plaisanterie qu'il a prononcée à sa retraite: «Les vieux professeurs ne meurent jamais, ils deviennent simplement émérites.» Sheffer est également crédité de l'expression «algèbre booléenne» (le sujet du chapitre 12 de ce texte). Sheffer a été brièvement marié et a vécu la plupart de sa vie plus tard dans de petites chambres dans un hôtel rempli de ses livres de logique et de vastes fichiers de bouts de papier qu'il utilisait pour noter son des idées. Malheureusement, Sheffer a souffert d'une grave dépression au cours des deux dernières décennies de sa vie.

c) Mei marche ou prend le bus pour aller en classe.
d) Ibrahim est intelligent et travaille dur.

8. Utilisez les lois de De Morgan pour trouver la négation de chacun des les déclarations suivantes.

a) Kwame occupera un emploi dans l'industrie ou obtiendra un diplôme école.
b) Yoshiko connaît Java et le calcul.
c) James est jeune et fort.
d) Rita déménagera en Oregon ou à Washington.

9. Montrez que chacune de ces déclarations conditionnelles est un en utilisant des tables de vérité.

a) $(p \land q) \to p$ **b)** $p \to (p \lor q)$
c) $\neg p \to (p \to q)$ **d)** $(p \land q) \to (p \to q)$
e) $\neg (p \to q) \to p$ **f)** $\neg (p \to q) \to \neg q$

10. Montrer que chacune de ces déclarations conditionnelles est un tau- en utilisant des tables de vérité.

a) $[\neg p \land (p \lor q)] \to q$
b) $[(p \to q) \land (q \to r)] \to (p \to r)$
c) $[p \land (p \to q)] \to q$
d) $[(p \lor q) \land (p \to r) \land (q \to r)] \to r$

11. Montrez que chaque énoncé conditionnel de l'exercice 9 est un tautologie sans utiliser de tables de vérité.

12. Montrez que chaque énoncé conditionnel de l'exercice 10 est un tautologie sans utiliser de tables de vérité.

13. Utilisez des tables de vérité pour vérifier les lois d'absorption.

a) $p \lor (p \land q) \equiv p$ **b)** $p \land (p \lor q) \equiv p$

14. Déterminez si $(\neg p \land (p \to q)) \to \neg q$ est une tautol- ogy.

15. Déterminez si $(\neg q \land (p \to q)) \to \neg p$ est une tautol- ogy.

Chacun des exercices 16-28 vous demande de montrer que deux composés les propositions sont logiquement équivalentes. Pour ce faire, soit montrer que les deux côtés sont vrais, ou que les deux côtés sont faux, pour exactement les mêmes combinaisons de valeurs de vérité de la propositionnelle variables dans ces expressions (selon ce qui est plus facile).

16. Montrer que $p \leftrightarrow q$ et $(p \land q) \lor (\neg p \land \neg q)$ sont logiquement équivalent.

17. Montrer que $\neg (p \leftrightarrow q)$ et $p \leftrightarrow \neg q$ sont logiquement équivalents prêté.

18. Montrer que $p \to q$ et $\neg q \to \neg p$ sont logiquement équivalents.

19. Montrez que $\neg p \leftrightarrow q$ et $p \leftrightarrow \neg q$ sont logiquement équivalents.

20. Montrer que $\neg (p \oplus q)$ et $p \leftrightarrow q$ sont logiquement équivalents.

21. Montrer que $\neg (p \leftrightarrow q)$ et $\neg p \leftrightarrow q$ sont logiquement équivalents prêté.

22. Montrer que $(p \to q) \land (p \to r)$ et $p \to (q \land r)$ sont log- iquement équivalents.

23. Montrer que $(p \to r) \land (q \to r)$ et $(p \lor q) \to r$ sont log- iquement équivalents.

24. Montrer que $(p \to q) \lor (p \to r)$ et $p \to (q \lor r)$ sont log- iquement équivalents.

25. Montrez que $(p \to r) \lor (q \to r)$ et $(p \land q) \to r$ sont log- iquement équivalents.

26. Montrer que $p \to (q \to r)$ et $q \to (p \lor r)$ sont logiquement équivalent.

27. Montrer que $p \leftrightarrow q$ et $(p \to q) \land (q \to p)$ sont logiquement équivalent.

28. Montrer que $p \leftrightarrow q$ et $\neg p \leftrightarrow \neg q$ sont logiquement équivalents.

29. Montrez que $(p \to q) \land (q \to r) \to (p \to r)$ est un tautol- ogy.

30. Montrez que $(p \lor q) \land (\neg p \lor r) \to (q \lor r)$ est une tautologie.

31. Montrez que $(p \to q) \to r$ et $p \to (q \to r)$ ne sont pas log- iquement équivalents.

32. Montrer que $(p \land q) \to r$ et $(p \to r) \land (q \to r)$ ne sont pas logiquement équivalent.

33. Montrer que $(p \to q) \to (r \to s)$ et $(p \to r) \to (q \to s)$ ne sont pas logiquement équivalents.

Le **dual** d'une proposition composée qui ne contient que le les opérateurs logiques ∨, ∧ et ¬ est la proposition composée obtenu en remplaçant chaque ∨ par ∧, chaque ∧ par ∨, chaque **T** par **F** , et chaque **F** par **T** . Le dual de s est noté s_* .

34. Trouvez le duel de chacune de ces propositions composées.

a) $p \lor \neg q$ **b)** $p \land (q \lor (r \land \mathbf{T}))$
c) $(p \land \neg q) \lor (q \land \mathbf{F})$

35. Trouvez le duel de chacune de ces propositions composées.

a) $p \land \neg q \land \neg r$ **b)** $(p \land q \land r) \lor s$
c) $(p \lor \mathbf{F}) \land (q \lor \mathbf{T})$

36. Quand $s_* = s$, où s est une proposition composée?

37. Montrer que $(s_*)_* = s$ lorsque s est une proposition composée.

38. Montrer que les équivalences logiques du tableau 6, à l'exception de la loi de la double négation, viennent par paires, où chaque paire contient des propositions composées qui sont doubles de chaque autre.

∗∗ 39. Pourquoi les doubles de deux composés équivalents proposent-ils

tions également équivalentes, où ces propositions composées ne contiennent que les opérateurs ∧ , ∨ et ¬?

40. Trouver une proposition composée impliquant la propositionnelle les variables p , q et r qui sont vraies lorsque p et q sont vraies et r est faux, mais est faux sinon. [*Astuce:* utilisez un jonction de chaque variable propositionnelle ou de sa négation.]

41. Trouver une proposition composée impliquant la propositionnelle les variables p, q et r qui sont vraies quand exactement deux de p, q , et r sont vrais et faux sinon. [*Astuce:* formez un disque jonction de conjonctions. Inclure une conjonction pour chacun combinaison de valeurs pour lesquelles le composé est vrai. Chaque conjonction doit inclure chacun des trois variables propositionnelles ou ses négations.]

42. Supposons qu'une table de vérité à n variables propositionnelles soit spécifié. Montrez qu'une proposition composée avec ce table de vérité peut être formée en prenant la disjonction de conjonctions des variables ou de leurs négations, avec une conjonction incluse pour chaque combinaison de valeurs pour dont la proposition composée est vraie. La résultante On dit que la proposition composée est en **nor- forme mal** .

Une collection d'opérateurs logiques est appelée **fonctionnellement com- plète** si chaque proposition est composé logiquement équivalent à une proposition composée impliquant uniquement ces opéra- tors.

43. Montrer que ¬, ∧ et ∨ forment une collection fonctionnellement complète sélection d'opérateurs logiques. [*Astuce:* utilisez le fait que chaque la proposition composée est logiquement équivalente à une forme normale disjonctive, comme illustré dans l'exercice 42.]

∗ **44.** Montrer que ¬ et ∧ forment une col-
sélection d'opérateurs logiques. [*Astuce:* utilisez d'abord un De Mor- loi générale pour montrer que $p \vee q$ est logiquement équivalent à $\neg(\neg p \wedge \neg q)$.]

∗ **45.** Montrer que ¬ et ∨ forment une collection fonctionnellement complète tion des opérateurs logiques.

Les exercices suivants impliquent les opérateurs logiques *NAND* et *NOR* . La proposition p *NAND* q est vraie lorsque p ou q , ou les deux, sont faux; et c'est faux quand p et q sont tous les deux vrai. La proposition p *NOR* q est vraie lorsque p et q sont tous deux faux, et c'est faux autrement. Les propositions p *NAND* q et p *NOR* q sont notés $p \mid q$ et $p \downarrow q$, respectivement. (Les opérateurs | et ↓ sont appelés le **trait de Sheffer** et le **Flèche Peirce** après HM Sheffer et CS Peirce, respectivement.)

46. Construisez une table de vérité pour l'opérateur logique *NAND* .

47. Montrez que $p \mid q$ est logiquement équivalent à $\neg(p \wedge q)$.

48. Construisez une table de vérité pour l'opérateur logique *NOR.*

49. Montrer que $p \downarrow q$ est logiquement équivalent à $\neg(p \vee q)$.

50. Dans cet exercice, nous montrerons que {↓} est fonctionnellement collection complète d'opérateurs logiques.

a) Montrer que $p \downarrow p$ est logiquement équivalent à $\neg p$.
b) Montrer que $(p \downarrow q) \downarrow (p \downarrow q)$ est logiquement équivalent à $p \vee q$.
c) Conclure des parties (a) et (b), et de l'exercice 49, que {↓} est une collection fonctionnelle complète de les opérateurs.

∗ **51.** Trouver une proposition composée logiquement équivalente à $p \rightarrow q$ *en* utilisant uniquement l'opérateur logique ↓.

52. Montrez que {|} est une collection fonctionnellement complète de opérateurs techniques.

53. Montrez que $p \mid q$ et $q \mid p$ sont équivalents.

54. Montrer que $p \mid (q \mid r)$ et $(p \mid q) \mid r$ ne sont pas équivalents, de sorte que l'opérateur logique | n'est pas associatif.

∗ **55.** Combien de tables de vérité différentes de propositions composées sont là qui impliquent les variables propositionnelles p et q ?

56. Montrer que si p , q et r sont des propositions composées telles que p et q sont logiquement équivalents et q et r sont logiquement équivalents, alors p et r sont logiquement équivalents.

57. La phrase suivante est tirée de la spécification de un système téléphonique: «Si la base de données d'annuaire est ouverte, alors le moniteur est mis dans un état fermé, si le système est pas dans son état initial. »Cette spécification est difficile à comprendre stand parce qu'il implique deux déclarations conditionnelles. Trouver une spécification équivalente et plus facile à comprendre qui volves disjonctions et négations mais pas conditionnelles déclarations.

58. Combien de disjonctions $p \vee \neg q$, $\neg p \vee q$, $q \vee r$, $q \vee \neg r$, et $\neg q \vee \neg r$ peuvent être rendus simultanément vrais par une affectation de valeurs de vérité à p , q et r ?

59. Combien de disjonctions $p \vee \neg q \vee s$, $\neg p \vee \neg r \vee s$, $\neg p \vee \neg r \vee \neg s$, $\neg p \vee q \vee \neg s$, $q \vee r \vee \neg s$, $q \vee \neg r \vee \neg s$, $\neg p \vee \neg q \vee \neg s$, $p \vee r \vee s$ et $p \vee r \vee \neg s$ peut être rendu simultanément vrai par une affectation de valeurs de vérité à p , q , r et s ?

60. Montrer que la négation d'un composé insatisfaisant proposition est une tautologie et la négation d'un composé proposition qui est une tautologie est insatisfaisante.

61. Déterminer si chacune de ces propositions composées est satisfaisable.

a) $(p \vee \neg q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q)$
b) $(p \rightarrow q) \wedge (p \rightarrow \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$
c) $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow q)$

62. Déterminer si chacune de ces propositions composées est satisfaisable.

a) $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$
b) $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$
c) $(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (\neg p \vee r \vee s) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee s) \wedge (\neg p \vee \neg r \vee \neg s)$

63. Montrez comment la solution d'un puzzle Sudoku 4 × 4 donné peut être trouvé en résolvant un problème de satisfiabilité.

64. Construire une proposition composée qui affirme que Chaque cellule d'un puzzle Sudoku 9 × 9 contient au moins un nombre.

65. Expliquez les étapes de la construction du complexe proposition donnée dans le texte qui affirme que chaque column d'un puzzle Sudoku 9 × 9 contient chaque nombre.

∗ **66.** Expliquez les étapes de la construction du complexe proposition donnée dans le texte qui affirme que chacun des neuf blocs 3 × 3 d'un puzzle Sudoku 9 × 9 contiennent des chaque numéro.

Prédicats et quantificateurs

introduction

La logique propositionnelle, étudiée dans les sections 1.1 à 1.3, ne peut pas exprimer correctement le sens de énoncés en mathématiques et en langage naturel.Par exemple, supposons que nous savons que

«Chaque ordinateur connecté au réseau universitaire fonctionne correctement.»

Aucune règle de logique propositionnelle ne nous permet de conclure à la vérité de l'énoncé

"MATH3 fonctionne correctement",

où MATH3 est l'un des ordinateurs connectés au réseau universitaire.De même, nous ne pouvons pas utiliser les règles de la logique propositionnelle pour conclure de la déclaration

"CS2 est attaqué par un intrus",

où CS2 est un ordinateur sur le réseau universitaire, pour conclure la vérité de

«Il y a un ordinateur sur le réseau universitaire qui est attaqué par un intrus.»

Dans cette section, nous présenterons un type de logique plus puissant appelé **logique de prédicat** . nous verront comment la logique des prédicats peut être utilisée pour exprimer la signification d'un large éventail d'instructions en mathématiques et en informatique d'une manière qui nous permet de raisonner et d'explorer les relations entre les objets. Pour comprendre la logique des prédicats, nous devons d'abord introduire le concept d'un prédicat. Ensuite, nous introduirons la notion de quantificateurs, qui nous permettent de raisonner avec des déclarations qui affirment qu'une certaine propriété est valable pour tous les objets d'un certain type et avec déclarations qui affirment l'existence d'un objet avec une propriété particulière.

Prédicats

Déclarations impliquant des variables, telles que

« $X > 3$. » « $x = y + 3$ », « $x + y = z$, »

et

"L'ordinateur x est attaqué par un intrus",

et

"L'ordinateur x fonctionne correctement",

se trouvent souvent dans les assertions mathématiques, dans les programmes informatiques et dans les spécifications du système. Ces déclarations ne sont ni vraies ni fausses lorsque les valeurs des variables ne sont pas spécifiées Dans Dans cette section, nous discuterons des façons de produire des propositions à partir de telles déclarations.

L'énoncé « x est supérieur à 3» comporte deux parties. La première partie, la variable x , est le sujet de la déclaration. La deuxième partie - le **prédicat** «est supérieur à 3» - fait référence à une propriété qui l'objet de la déclaration peut avoir. On peut noter l'énoncé « x est supérieur à 3» par $P(x)$, où P désigne le prédicat «est supérieur à 3» et x est la variable. La déclaration $P(x)$ est dit également être la valeur de la **fonction propositionnelle** P en x . Une fois qu'une valeur a été affectée à la variable x , l'énoncé $P(x)$ devient une proposition et a une valeur de vérité. Considérer Exemples 1 et 2.

EXEMPLE 1 Soit $P(x)$ la phrase « $x > 3$.» Quelles sont les valeurs de vérité de $P(4)$ et $P(2)$?

Solution: Nous obtenons l'énoncé $P(4)$ en définissant $x = 4$ dans l'énoncé « $x > 3$.». Par conséquent, $P(4)$, qui est l'énoncé « $4 > 3$ », est vrai. Cependant, $P(2)$, qui est la déclaration « $2 > 3$ », c'est faux. ▲

EXEMPLE 2 Soit $A(x)$ la phrase «l'ordinateur x est attaqué par un intrus». Supposons que celle du ordinateurs sur le campus, seuls CS2 et MATH1 sont actuellement attaqués par des intrus. Quels sont valeurs de vérité de A (CS1), A (CS2) et A (MATH1)?

Solution: Nous obtenons l'instruction A (CS1) en définissant x = CS1 dans l'instruction «Computer x est attaqué par un intrus. "Parce que CS1 n'est pas sur la liste des ordinateurs actuellement sous attaque, nous concluons que A (CS1) est faux. De même, parce que CS2 et MATH1 sont sur la liste des les ordinateurs attaqués, nous savons que A (CS2) et A (MATH1) sont vrais. ▲

Nous pouvons également avoir des instructions qui impliquent plus d'une variable. Par exemple, considérez le déclaration « $x = y + 3$.» Nous pouvons désigner cette déclaration par $Q(x, y)$, où x et y sont des variables et Q est le prédicat. Lorsque des valeurs sont affectées aux variables x et y , l'instruction $Q(x, y)$

a une valeur de vérité.

EXEMPLE 3 Soit $Q(x, y)$ la phrase « $x = y + 3$». Quelles sont les valeurs de vérité des propositions $Q(1, 2)$ et $Q(3, 0)$?

Solution: Pour obtenir $Q(1, 2)$, définissez $x = 1$ et $y = 2$ dans l'instruction $Q(x, y)$. Par conséquent, $Q(1, 2)$ est l'énoncé «$1 = 2 + 3$», qui est faux.L'énoncé $Q(3, 0)$ est la proposition «$3 = 0 + 3$» ce qui est vrai. ▲

CHARLES SANDERS PEIRCE (1839–1914) Beaucoup considèrent Charles Peirce, né à Cambridge, Massachusetts, pour être l'intellect américain le plus original et le plus polyvalent. Il a apporté une contribution importante à nombre incroyable de disciplines, dont les mathématiques, l'astronomie, la chimie, la géodésie, la métrologie, ingénierie, psychologie, philologie, histoire des sciences et économie. Peirce était aussi un inventeur, un étudiant à vie de la médecine, un critique de livre, un dramaturge et un acteur, un écrivain de nouvelles, un phénoménologue, un logicien et un métaphysicien. Il est noté comme le philosophe éminent de la construction de systèmes compétent et productif en logique, mathématiques et un large éventail de sciences. Il a été encouragé par son père, Benjamin Peirce, professeur de mathématiques et philosophie naturelle à Harvard, pour poursuivre une carrière scientifique. Au lieu de cela, il a décidé d'étudier la logique et méthodologie scientifique. Peirce fréquente Harvard (1855–1859) et obtient une maîtrise ès arts de Harvard (1862) et un diplôme d'études supérieures en chimie de la Lawrence Scientific School (1863).
En 1861, Peirce est devenu assistant au US Coast Survey, dans le but de mieux comprendre la méthodologie scientifique. Son service car l'enquête l'exempte du service militaire pendant la guerre civile. Tout en travaillant pour le levé, Peirce a fait des études astronomiques et travaux géodésiques. Il a apporté des contributions fondamentales à la conception des pendules et à la cartographie des projections, en appliquant de nouvelles développements dans la théorie des fonctions elliptiques. Il a été la première personne à utiliser la longueur d'onde de la lumière comme unité de mesure. Peirce accède au poste d'assistant pour l'enquête, poste qu'il occupe jusqu'à ce qu'il soit contraint de démissionner en 1891, lorsqu'il n'est pas d'accord avec le direction prise par la nouvelle administration de l'Enquête.

Tout en gagnant sa vie du travail dans les sciences physiques, Peirce a développé une hiérarchie des sciences, avec les mathématiques à la échelon supérieur, dans lequel les méthodes d'une science pourraient être adaptées pour être utilisées par les sciences qui la composent dans la hiérarchie. Pendant ce temps, il a également fondé la théorie philosophique américaine du pragmatisme.

Le seul poste académique que Peirce ait jamais occupé a été professeur de logique à l'Université Johns Hopkins de Baltimore (1879–1884). Le sien le travail mathématique durant cette période comprenait des contributions à la logique, à la théorie des ensembles, à l'algèbre abstraite et à la philosophie des mathématiques. Son travail est toujours d'actualité aujourd'hui, avec des applications récentes de ce travail sur la logique à l'intelligence artificielle. Peirce croyait que l'étude des mathématiques pourraient développer les pouvoirs d'imagination, d'abstraction et de généralisation de l'esprit. Ses diverses activités après sa retraite de l'enquête comprenait la rédaction de périodiques, la contribution à des dictionnaires savants, la traduction d'articles scientifiques, des conférences, et rédaction de manuels. Malheureusement, ses revenus provenant de ces poursuites étaient insuffisants pour le protéger, lui et sa deuxième épouse, la pauvreté. Il a été soutenu dans ses dernières années par un fonds créé par ses nombreux admirateurs et administré par le philosophe William James, son ami de toujours. Bien que Peirce ait écrit et publié de manière volumineuse dans une vaste gamme de sujets, il a laissé plus de 100 000 pages de manuscrits non publiés. En raison de la difficulté d'étudier ses écrits non publiés, les chercheurs n'ont commencé que récemment pour comprendre certaines de ses contributions variées. Un groupe de personnes se consacre à rendre son travail disponible sur Internet pour apporter une meilleure appréciation des réalisations de Peirce dans le monde.

EXEMPLE 4 Soit $A(c, n)$ la phrase «l'ordinateur c est connecté au réseau n », où c est une variable représentant un ordinateur et n est une variable représentant un réseau.Supposons que l'ordinateur MATH1 est connecté au réseau CAMPUS2, mais pas au réseau CAMPUS1.Quels sont les valeurs de A (MATH1, CAMPUS1) et A (MATH1, CAMPUS2)?

Solution: MATH1 n'étant pas connecté au réseau CAMPUS1, nous constatons que A (MATH1, CAMPUS1) est faux. Cependant, comme MATH1 est connecté au réseau CAMPUS2, nous voir que A (MATH1, CAMPUS2) est vrai. ▲

De même, nous pouvons laisser $R(x, y, z)$ désigner l'énoncé « $x + y = z$ ». Lorsque des valeurs sont attribuées pour les variables x, y et z, cette déclaration a une valeur de vérité.

EXEMPLE 5 Quelles sont les valeurs de vérité des propositions $R(1, 2, 3)$ et $R(0, 0, 1)$?

Solution: La proposition $R(1, 2, 3)$ est obtenue en fixant $x = 1$, $y = 2$ et $z = 3$ dans le instruction $R(x, y, z)$. Nous voyons que $R(1, 2, 3)$ est l'énoncé «$1 + 2 = 3$», ce qui est vrai.Aussi notez que $R(0, 0, 1)$, qui est l'énoncé «$0 + 0 = 1$», est faux. ▲

En général, une instruction impliquant les n variables $x_1, x_2, \ldots, x_n$ peut être notée par

$$P(x_1, x_2, \ldots, x_n).$$

Un énoncé de la forme $P(x_1, x_2, \ldots, x_n)$ est la valeur de la **fonction propositionnelle** P à la n uplet $(x_1, x_2, \ldots, x_n)$, et P est également appelé n **-Place prédicat** ou un n **prédicat -aire** .

Les fonctions propositionnelles se produisent dans les programmes informatiques, comme le montre l'exemple 6.

EXEMPLE 6 Considérez la déclaration

si $x > 0$ **alors** $x := x + 1$.

Lorsque cette instruction est rencontrée dans un programme, la valeur de la variable x à ce point dans le l'exécution du programme est insérée dans $P(x)$, qui est « $x > 0$». Si $P(x)$ est vrai pour cette valeur de x , l'instruction d'affectation $x := x + 1$ est exécutée, donc la valeur de x est augmentée de 1. Si $P(x)$ est faux pour cette valeur de x , l'instruction d'affectation n'est pas exécutée, donc la valeur de x est inchangé. ▲

PRÉCONDITIONS ET POSTCONDITIONS Les prédicats sont également utilisés pour l'exactitude des programmes informatiques, c'est-à-dire pour montrer que les programmes informatiques produisent sortie souhaitée lorsque l'entrée est valide. (Notez qu'à moins que l'exactitude d'un programme informatique est établi, aucun test ne peut montrer qu'il produit la sortie souhaitée pour toutes les entrées , sauf si chaque valeur d'entrée est testée.) Les instructions qui décrivent une entrée valide sont connues comme **conditions préalables** et conditions que la sortie doit remplir lorsque le programme est exécuté sont connus comme **postconditions** . Comme l'illustre l'exemple 7, nous utilisons des prédicats pour décrire les deux conditions préalables et postconditions. Nous étudierons ce processus plus en détail dans la section 5.5.

EXEMPLE 7 Considérons le programme suivant, conçu pour échanger les valeurs de deux variables x et y .

```
temp: = x
x: = y
y: = temp
```

Trouver des prédicats que nous pouvons utiliser comme condition préalable et postcondition pour vérifier l'exactitude de ce programme. Expliquez ensuite comment les utiliser pour vérifier que pour toute entrée valide le programme ce qui est prévu.

Solution: Pour la condition préalable, nous devons exprimer que x et y ont des valeurs particulières avant nous exécutons le programme. Donc, pour cette condition préalable, nous pouvons utiliser le prédicat $P(x, y)$, où $P(x, y)$ est la déclaration « $x = a$ et $y = b$ », où a et b sont les valeurs de x et y avant d'exécuter le programme. Parce que nous voulons vérifier que le programme échange les valeurs de x et y pour toutes les entrées valeurs, pour la postcondition, nous pouvons utiliser $Q(x, y)$, où $Q(x, y)$ est la déclaration « $x = b$ et $y = a$. "

Pour vérifier que le programme fait toujours ce qu'il est censé faire, supposons que la précon- la position $P(x, y)$ est vraie. Autrement dit, nous supposons que l'énoncé « $x = a$ et $y = b$ » est vrai. Cette signifie que $x = a$ et $y = b$. La première étape du programme, $temp := x$, affecte la valeur de x à la variable *temp* , donc après cette étape, nous savons que $x = a$, $temp = a$ et $y = b$. Après la seconde étape du programme, $x := y$, nous savons que $x = b$, $temp = a$ et $y = b$. Enfin, après le troisième étape, nous savons que $x = b$, $temp = a$ et $y = a$. Par conséquent, après l'exécution de ce programme, le postcondition $Q(x, y)$ tient, c'est-à-dire que la déclaration « $x = b$ et $y = a$ » est vraie. ▲

Quantificateurs

Lorsque les variables d'une fonction propositionnelle reçoivent des valeurs, l'instruction résultante devient une proposition avec une certaine valeur de vérité. Cependant, il existe un autre moyen important, appelé **quantification** , pour créer une proposition à partir d'une fonction propositionnelle. La quantification exprime la mesure dans laquelle un prédicat est vrai sur une gamme d'éléments. En anglais, les mots *all* , *some* , *beaucoup* , *aucun* et *peu* sont utilisés dans les quantifications. Nous nous concentrerons sur deux types de quantification ici: quantification universelle, qui nous dit qu'un prédicat est vrai pour chaque élément sous considération, et quantification existentielle, qui nous dit qu'il y a un ou plusieurs éléments à l'étude pour laquelle le prédicat est vrai. Le domaine de la logique qui traite des prédicats et les quantificateurs est appelé le **calcul des prédicats** .

LE QUANTIFIANT UNIVERSEL De nombreux énoncés mathématiques affirment qu'une propriété est vrai pour toutes les valeurs d'une variable dans un domaine particulier, appelé **domaine du discours** (ou l' **univers du discours**), souvent appelé simplement le **domaine** . Une telle déclaration est exprimée en utilisant la quantification universelle. La quantification universelle de $P(x)$ pour un domaine particulier est la proposition qui affirme que $P(x)$ est vrai pour toutes les valeurs de x dans ce domaine. Notez que le domaine spécifie les valeurs possibles de la variable x . Le sens de la quantification universelle de $P(x)$ change lorsque nous changeons de domaine. Le domaine doit toujours être spécifié lorsqu'un quantificateur universel est utilisé; sans elle, la quantification universelle d'un énoncé n'est pas définie.

DÉFINITION 1 La *quantification universelle* de $P(x)$ est la déclaration

" $P(x)$ pour toutes les valeurs de x dans le domaine."

La notation $\forall x P(x)$ indique la quantification universelle de $P(x)$. Ici $\forall$ est appelé **quantificateur universel.** Nous lisons $\forall x P(x)$ comme «pour tous les $x P(x)$ » ou «pour tous les $x P(x)$ ». Un élément pour lequel $P(x)$ est faux est appelé un **contre - exemple** de $\forall x P(x)$.

La signification du quantificateur universel est résumée dans la première ligne du tableau 1. Nous illustrent l'utilisation du quantificateur universel dans les exemples 8 à 13.

TABLEAU 1 Quantificateurs.

Déclaration	*Quand c'est vrai?*	*Quand est-ce faux?*
$\forall x P(x)$	$P(x)$ est vrai pour chaque x .	Il y a un x pour lequel $P(x)$ est faux.
$\exists x P(x)$	Il y a un x pour lequel $P(x)$ est vrai.	$P(x)$ est faux pour chaque x.

EXEMPLE 8 Soit $P(x)$ l'énoncé « $x + 1 > x$ ». Quelle est la valeur de vérité de la quantification $\forall x P(x)$, où le domaine se compose de tous les nombres réels?

Solution: Parce que $P(x)$ est vrai pour tous les nombres réels x , la quantification

$$\forall x P(x)$$

est vrai. ▲

Remarque: Généralement, une hypothèse implicite est faite que tous les domaines du discours pour les quantificateurs sont non vides. Notez que si le domaine est vide, alors $\forall x P(x)$ est vrai pour toute propositionnelle fonction $P(x)$ car il n'y a pas d'éléments x dans le domaine pour lesquels $P(x)$ est faux.

N'oubliez pas que la vérité la valeur de $\forall x P(x)$ dépend sur le domaine!

Outre «pour tous» et «pour tous», la quantification universelle peut être exprimée dans de nombreux autres différentes manières, y compris «tous», «pour chacun», «compte tenu de tout», «pour arbitraire», «pour chacun» et «pour tout».

Remarque: Il est préférable d'éviter d'utiliser «pour tout x » car il est souvent ambigu de savoir si «tout» signifie «tous» ou «certains». Dans certains cas, «tout» est sans ambiguïté, comme lorsqu'il est utilisé dans les négatifs, par exemple, "il n'y a aucune raison d'éviter d'étudier."

Une déclaration $\forall x P(x)$ est fausse, où $P(x)$ est une fonction propositionnelle, si et seulement si $P(x)$ n'est pas toujours vrai lorsque x est dans le domaine. Une façon de montrer que $P(x)$ n'est pas toujours vrai lorsque x est dans le est de trouver un contre-exemple à l'instruction $\forall x P(x)$. Notez qu'un seul contre-exemple est tout ce dont nous avons besoin pour établir que $\forall x P(x)$ est faux. L'exemple 9 illustre comment les contre-exemples sont utilisés.

EXEMPLE 9 Soit $Q(x)$ l'énoncé « $x < 2$.» Quelle est la valeur de vérité de la quantification $\forall x Q(x)$, où le domaine est composé de tous les nombres réels?

Solution: $Q(x)$ n'est pas vrai pour chaque nombre réel x , car, par exemple, $Q(3)$ est faux. C'est, $x = 3$ est un contre-exemple pour l'instruction $\forall x Q(x)$. Donc

$$\forall x Q(x)$$

c'est faux. ▲

EXEMPLE 10 Supposons que $P(x)$ soit « $x^2 > 0$». Pour montrer que la déclaration $\forall x P(x)$ est fausse où l'univers du discours se compose de tous les entiers, nous donnons un contre-exemple. On voit que $x = 0$ est un contre-exemple car $x^2 = 0$ lorsque $x = 0$, de sorte que x^2 n'est pas supérieur à 0 lorsque $x = 0$. ▲

La recherche de contre-exemples d'énoncés universellement quantifiés est une activité importante dans l'étude des mathématiques, comme nous le verrons dans les sections suivantes de ce livre.

Lorsque tous les éléments du domaine peuvent être répertoriés (disons $x_1, x_2, \ldots, x_n$), il s'ensuit que le quantification universelle $\forall x P(x)$ est la même que la conjonction

$$P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n),$$

car cette conjonction est vraie si et seulement si $P(x_1), P(x_2), \ldots, P(x_n)$ sont tous vrais.

EXEMPLE 11 Quelle est la valeur de vérité de $\forall x P(x)$, où $P(x)$ est l'énoncé « $x^2 < 10$» et le domaine se compose des entiers positifs ne dépassant pas 4?

Solution: l'instruction $\forall x P(x)$ est la même que la conjonction

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4),$$

parce que le domaine se compose des entiers 1, 2, 3 et 4. Parce que $P(4)$, qui est la déclaration «$4^2 < 10$» est faux, il s'ensuit que $\forall x P(x)$ est faux. ▲

EXEMPLE 12 Que signifie la déclaration $\forall x N(x)$ si $N(x)$ est «l'ordinateur x est connecté au réseau» et le domaine se compose de tous les ordinateurs sur le campus?

Solution: L'instruction $\forall x N(x)$ signifie que pour chaque ordinateur x sur le campus, cet ordinateur x est connecté au réseau. Cette déclaration peut être exprimée en anglais sous la forme «Chaque ordinateur le campus est connecté au réseau. ▲

Comme nous l'avons souligné, la spécification du domaine est obligatoire lorsque des quantificateurs sont utilisés. le La valeur de vérité d'une déclaration quantifiée dépend souvent des éléments qui se trouvent dans ce domaine, comme L'exemple 13 montre.

EXEMPLE 13 Quelle est la valeur de vérité de $\forall x (x^2 \geq x)$ si le domaine est composé de tous les nombres réels? Quel est le valeur de vérité de cette déclaration si le domaine se compose de tous les entiers?

Solution: la quantification universelle $\forall x (x^2 \geq x)$, où le domaine se compose de tous les nombres réels bers, est faux. Par exemple, $(\frac{1}{2})^2 \geq \frac{1}{2}$. Notez que $x^2 \geq x$ si et seulement si $x^2 - x = x(x - 1) \geq 0$. Par conséquent, $x^2 \geq x$ si et seulement si $x \leq 0$ ou $x \geq 1$. Il s'ensuit que $\forall x (x^2 \geq x)$ est faux si le Le domaine se compose de tous les nombres réels (car l'inégalité est fausse pour tous les nombres réels x avec $0 < x < 1$). Cependant, si le domaine se compose des entiers, $\forall x (x^2 \geq x)$ est vrai, car il ne sont pas des entiers x avec $0 < x < 1$. ▲

LE QUANTIFICATEUR EXISTENTIEL De nombreux énoncés mathématiques affirment qu'il existe un élément avec une certaine propriété. Ces déclarations sont exprimées en utilisant une quantification existentielle. Avec la quantification existentielle, nous formons une proposition qui est vraie si et seulement si $P(x)$ est vraie pour au moins une valeur de x dans le domaine.

DÉFINITION 2 La *quantification existentielle* de $P(x)$ est la proposition

"Il existe un élément x dans le domaine tel que $P(x)$."

Nous utilisons la notation $\exists x P(x)$ pour la quantification existentielle de $P(x)$. Ici $\exists$ est appelé *quantificateur existentiel*.

Un domaine doit toujours être spécifié lorsqu'une instruction $\exists x P(x)$ est utilisée. En outre, le la signification de $\exists x P(x)$ change lorsque le domaine change. Sans spécifier le domaine, le l'instruction $\exists x P(x)$ n'a pas de sens.

Outre l'expression «il existe», nous pouvons également exprimer la quantification existentielle dans de nombreux autres différentes manières, par exemple en utilisant les mots «pour certains», «pour au moins un» ou «il y en a». la quantification $\exists x P(x)$ se lit comme

"Il y a un x tel que $P(x)$,"
"Il y a au moins un x tel que $P(x)$,"

ou

"Pour certains $x P(x)$."

La signification du quantificateur existentiel est résumée dans la deuxième ligne du tableau 1. Nous illustrent l'utilisation du quantificateur existentiel dans les exemples 14 à 16.

EXEMPLE 14 Soit $P(x)$ la phrase « $x > 3$.» Quelle est la valeur de vérité de la quantification $\exists x P(x)$, où le domaine se compose de tous les nombres réels?

Solution: Parce que « $x > 3$» est parfois vrai - par exemple, lorsque $x = 4$ - le quantum existentiel tification de $P(x)$, qui est $\exists x P(x)$, est vraie. ▲

Observez que l'instruction $\exists x P(x)$ est fausse si et seulement s'il n'y a pas d'élément x dans le domaine pour lequel $P(x)$ est vrai. Autrement dit, $\exists x P(x)$ est faux si et seulement si $P(x)$ est faux pour chaque élément de le domaine. Nous illustrons cette observation dans l'exemple 15.

EXEMPLE 15 Soit $Q(x)$ la phrase « $x = x + 1$». Quelle est la valeur de vérité de la quantification $\exists x Q(x)$, où le domaine se compose de tous les nombres réels?

Solution: Parce que $Q(x)$ est faux pour chaque nombre réel x, la quantification existentielle de $Q(x)$, qui est $\exists x Q(x)$, est faux. ▲

N'oubliez pas que la vérité la valeur de $\exists x P(x)$ dépend sur le domaine!

Remarque: Généralement, une hypothèse implicite est faite que tous les domaines du discours pour les quantificateurs sont non vides. Si le domaine est vide, alors $\exists x Q(x)$ est faux chaque fois que $Q(x)$ est une propositionnelle fonction parce que lorsque le domaine est vide, il ne peut y avoir d'élément x dans le domaine pour lequel $Q(x)$ est vrai.

Lorsque tous les éléments du domaine peuvent être répertoriés - disons, $x_1, x_2, \ldots, x_n$ - le quan-*tification* $\exists x P(x)$ est la même que la disjonction

$$P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n),$$

car cette disjonction est vraie si et seulement si au moins l'un de $P(x_1), P(x_2), \ldots, P(x_n)$ est vrai.

EXEMPLE 16 Quelle est la valeur de vérité de $\exists x P(x)$, où $P(x)$ est l'énoncé « $x^2 > 10$» et l'univers de le discours consiste en des entiers positifs ne dépassant pas 4?

Solution: comme le domaine est $\{1, 2, 3, 4\}$, la proposition $\exists x P(x)$ est la même que la disjonction tion

$$P(1) \vee P(2) \vee P(3) \vee P(4).$$

Puisque $P(4)$, qui est l'énoncé « $4^2 > 10$», est vrai, il s'ensuit que $\exists x P(x)$ est vrai. ▲

Il est parfois utile de penser en termes de boucle et de recherche lors de la détermination du valeur de vérité d'une quantification. Supposons qu'il y ait n objets dans le domaine pour la variable x. Pour déterminer si $\forall x P(x)$ est vrai, nous pouvons parcourir toutes les n valeurs de x pour voir si $P(x)$ est toujours vrai. Si nous rencontrons une valeur x pour laquelle $P(x)$ est fausse, alors nous avons montré que $\forall x P(x)$ est faux. Sinon, $\forall x P(x)$ est vrai. Pour voir si $\exists x P(x)$ est vrai, nous *parcourons* les n valeurs de x recherchant une valeur pour laquelle $P(x)$ est vraie. Si nous en trouvons un, alors $\exists x P(x)$ est vrai. Si nous ne trouvons jamais un tel x, alors nous avons déterminé que $\exists x P(x)$ est faux. (Notez que ce la procédure de recherche ne s'applique pas s'il existe une infinité de valeurs dans le domaine. cependant, c'est encore une façon utile de penser aux valeurs de vérité des quantifications.)

LE QUANTIFIANT D'UNICITÉ Nous avons maintenant introduit des quantificateurs. Ce sont les quantificateurs les plus importants en mathématiques et en informatique.cependant, il n'y a pas de limitation sur le nombre de quantificateurs différents que nous pouvons définir, comme «il y a exactement deux »,« il n'y en a pas plus de trois »,« il y en a au moins 100 », etcDe ces autres quantificateurs, celui qui est le plus souvent vu est le**quantificateur d'unicité** , noté ∃! ou $\exists_1$.
La notation $\exists! xP(x)$ [ou $\exists_1 xP(x)$] indique "Il existe un$x$ unique tel que $P(x)$ soit vrai." (D'autres expressions pour la quantification de l'unicité incluent «il y en a exactement un» et «il y en a un et un seul. ») Par exemple, $\exists! x(x - 1 = 0)$, où le domaine est l'ensemble des nombres réels, indique qu'il existe un nombre réel unique$x$ tel que $x - 1 = 0$. Ceci est une vraie déclaration, car$x = 1$ est le nombre réel unique tel que$x - 1 = 0$. Remarquez que nous pouvons utiliser des quantificateurs et des propositions logique pour exprimer l'unicité (voir l'exercice 52 dans la section 1.5), de sorte que le quantificateur d'unicité peut être évité. En règle générale, il est préférable de s'en tenir aux quantificateurs existentiels et universels pour que les règles d'inférence pour ces quantificateurs peuvent être utilisés.

Quantificateurs avec domaines restreints

Une notation abrégée est souvent utilisée pour restreindre le domaine d'un quantificateur. Dans cette notation, une condition à laquelle une variable doit satisfaire est incluse après le quantificateur.Ceci est illustré dans Exemple 17. Nous décrirons également d'autres formes de cette notation impliquant l'appartenance à un ensemble dans Section 2.1.

EXEMPLE 17 Que signifient les instructions $\forall x < 0\ (x^2 > 0)$, $\forall y \neq 0\ (y^3 \neq 0)$ et $\exists z > 0\ (z^2 = 2)$, où le domaine dans chaque cas se compose des nombres réels?

Solution: L'instruction$\forall x < 0\ (x^2 > 0)$ indique que pour chaque nombre réel x avec $x < 0$, $x^2 > 0$. Autrement dit, il indique «Le carré d'un nombre réel négatif est positif». Cette déclaration est la même comme $\forall x(x < 0 \rightarrow x^2 > 0)$.

L'instruction $\forall y \neq 0\ (y^3 \neq 0)$ indique que pour chaque nombre réel y avec $y \neq 0$, nous avons $y^3 \neq 0$. Autrement dit, il indique que "le cube de chaque nombre réel non nul est différent de zéro". Notez que ce est équivalente à $\forall y(y \neq 0 \rightarrow y^3 \neq 0)$.

Enfin, l'énoncé $\exists z > 0\ (z^2 = 2)$ indique qu'il existe un nombre réel$z$ avec $z > 0$ tel que $z^2 = 2$. Autrement dit, il indique "Il y a une racine carrée positive de 2." Cette déclaration est équivalent à $\exists z(z > 0 \wedge z^2 = 2)$. ▲

Notez que la restriction d'une quantification universelle est la même que la quantification universelle cation d'une déclaration conditionnelle. Par exemple, $\forall x < 0\ (x^2 > 0)$ est une autre façon d'exprimer $\forall x(x < 0 \rightarrow x^2 > 0)$. D'autre part, la restriction d'une quantification existentielle est la même que la quantification existentielle d'une conjonction. Par exemple, $\exists z > 0\ (z^2 = 2)$ est un autre manière d'exprimer $\exists z(z > 0 \wedge z^2 = 2)$.

Priorité des quantificateurs

Les quantificateurs ∀ et ∃ ont une priorité plus élevée que tous les opérateurs logiques de propositionnelle calcul. Par exemple, $\forall xP(x) \vee Q(x)$ est la disjonction de $\forall xP(x)$ et $Q(x)$. En d'autres termes, cela signifie $(\forall xP(x)) \vee Q(x)$ plutôt que $\forall x(P(x) \vee Q(x))$.

Variables de liaison

Lorsqu'un quantificateur est utilisé sur la variable$x$, nous disons que cette occurrence de la variable est**liée** . Une occurrence d'une variable qui n'est pas liée par un quantificateur ou un ensemble égal à une valeur particulière est dit **gratuit** . Toutes les variables qui se produisent dans une fonction propositionnelle doivent être liées ou définies égale à une valeur particulière pour en faire une proposition.Cela peut être fait en utilisant une combinaison de quantificateurs universels, quantificateurs existentiels et attributions de valeurs.

La partie d'une expression logique à laquelle un quantificateur est appliqué est appelée la **portée** de cette quantificateur. Par conséquent, une variable est libre si elle est hors de la portée de tous les quantificateurs du formule qui spécifie cette variable.

EXEMPLE 18 Dans l'instruction $\exists x (x + y = 1)$, la variable x est liée par la quantification existentielle $\exists x$, mais la variable y est libre car elle n'est pas liée par un quantificateur et aucune valeur n'est affectée à cette variable variable. Cela illustre que dans l'instruction $\exists x (x + y = 1)$, x est lié, mais y est libre.

Dans l'instruction statement $x (P (x) \wedge Q (x)) \vee \forall xR (x)$, toutes les variables sont liées. La portée du premier quantificateur, $\exists x$, est l'expression $P (x) \wedge Q (x)$ car $\exists x$ est appliqué uniquement à $P (x) \wedge Q (x)$, et pas au reste de la déclaration. De même, la portée du deuxième quantificateur, $\forall x$, est l'expression $R (x)$. Autrement dit, le quantificateur existentiel lie la variable x dans $P (x) \wedge Q (x)$ et l'universel le quantificateur $\forall x$ lie la variable x dans $R (x)$. Notez que nous aurions pu écrire notre déclaration en utilisant deux variables différentes x et y , comme $\exists x (P (x) \wedge Q (x)) \vee \forall yR (y)$, car les portées de les deux quantificateurs ne se chevauchent pas. Le lecteur doit être conscient que dans l'usage courant, le même lettre est souvent utilisée pour représenter des variables liées par différents quantificateurs avec des étendues qui ne chevauchement. ▲

Équivalences logiques impliquant des quantificateurs

Dans la section 1.3, nous avons introduit la notion d'équivalences logiques des propositions composées. nous peut étendre cette notion à des expressions impliquant des prédicats et des quantificateurs.

DÉFINITION 3 Les déclarations impliquant des prédicats et des quantificateurs sont *logiquement équivalentes* si et seulement si elles ont la même valeur de vérité, peu importe quels prédicats sont substitués dans ces déclarations et quel domaine du discours est utilisé pour les variables de ces fonctions propositionnelles. Nous utilisons la notation $S \equiv T$ pour indiquer que deux déclarations S et T impliquant des prédicats et les quantificateurs sont logiquement équivalents.

L'exemple 19 illustre comment montrer que deux instructions impliquant des prédicats et des quantificateurs sont logiquement équivalents.

EXEMPLE 19 Montrer que $\forall x (P (x) \wedge Q (x))$ et $\forall xP (x) \wedge \forall xQ (x)$ sont logiquement équivalents (où les mêmes est utilisé partout). Cette équivalence logique montre que nous pouvons distribuer un universel quantificateur sur une conjonction. De plus, nous pouvons également distribuer un quantificateur existentiel sur une disjonction. Cependant, nous ne pouvons pas distribuer un quantificateur universel sur une disjonction, ni nous distribuons un quantificateur existentiel sur une conjonction. (Voir les exercices 50 et 51.)

Solution: pour montrer que ces déclarations sont logiquement équivalentes, nous devons montrer qu'elles sont toujours prendre la même valeur de vérité, quels que soient les prédicats P et Q , et quel que soit domaine du discours est utilisé. Supposons que nous ayons des prédicats particuliers P et Q , avec un commun domaine. On peut montrer que $\forall x (P (x) \wedge Q (x))$ et $\forall xP (x) \wedge \forall xQ (x)$ sont logiquement équivalents en faisant deux choses. Tout d'abord, nous montrons que si $\forall x (P (x) \wedge Q (x))$ est vrai, alors $\forall xP (x) \wedge \forall xQ (x)$ est vrai. Deuxièmement, nous montrons que si $\forall xP (x) \wedge \forall xQ (x)$ est vrai, alors $\forall x (P (x) \wedge Q (x))$ est vrai.

Supposons donc que $\forall x (P (x) \wedge Q (x))$ soit vrai. Cela signifie que si a est dans le domaine, alors $P (a) \wedge Q (a)$ est vrai. Par conséquent, $P (a)$ est vrai et $Q (a)$ est vrai. Parce que $P (a)$ est vrai et $Q (a)$ est vrai pour chaque élément du domaine, nous pouvons conclure que $\forall xP (x)$ et $\forall xQ (x)$ sont tous les deux vrais. Cela signifie que $\forall xP (x) \wedge \forall xQ (x)$ est vrai.

Supposons ensuite que $\forall xP (x) \wedge \forall xQ (x)$ est vrai. Il s'ensuit que $\forall xP (x)$ est vrai et $\forall xQ (x)$ est vrai. Par conséquent, si a est dans le domaine, alors $P (a)$ est vrai et $Q (a)$ est vrai [parce que $P (x)$ et $Q (x)$ sont tous les deux vrais pour tous les éléments du domaine, il n'y a pas de conflit en utilisant la même valeur *que* ici].

Il s'ensuit que pour tout a , $P (a) \wedge Q (a)$ est vrai. Il s'ensuit que $\forall x (P (x) \wedge Q (x))$ est vrai. nous pouvons conclure maintenant que

$$\forall x (P (x) \wedge Q (x)) \equiv \forall xP (x) \wedge \forall xQ (x).$$ ▲

Négation d'expressions quantifiées

Nous voudrons souvent considérer la négation d'une expression quantifiée. Par exemple, considérez la négation de la déclaration

"Chaque élève de votre classe a suivi un cours de calcul."

Cette déclaration est une quantification universelle, à savoir,

$\forall x P(x)$,

où $P(x)$ est l'énoncé « x a suivi un cours de calcul» et le domaine se compose des les élèves de votre classe. La négation de cette affirmation est: «Il n'est pas vrai que chaque élève votre classe a suivi un cours de calcul ». Cela équivaut à« Il y a un élève dans votre classe qui n'a pas suivi de cours de calcul. »Et il s'agit simplement de la quantification existentielle de la négation de la fonction propositionnelle d'origine, à savoir,

$\exists x \neg P(x)$.

Cet exemple illustre l'équivalence logique suivante:

$$\neg \forall x P(x) \equiv \exists x \neg P(x).$$

Pour montrer que $\neg \forall x P(x)$ et $\exists x P(x)$ sont logiquement équivalents quelle que soit la proposition fonction $P(x)$ et quel est le domaine, notons d'abord que $\neg \forall x P(x)$ est vrai si et seulement si $\forall x P(x)$ est faux. Ensuite, notez que $\forall x P(x)$ est faux si et seulement s'il y a un élément x dans le domaine pour lequel $P(x)$ est faux. Cela vaut si et seulement s'il y a un élément x dans le domaine pour lequel $\neg P(x)$ est vrai. Enfin, notons qu'il existe un élément x dans le domaine pour lequel $\neg P(x)$ est vrai si et seulement si $\exists x \neg P(x)$ est vrai. En rassemblant ces étapes, nous pouvons conclure que $\neg \forall x P(x)$ est vrai si et seulement si $\exists x \neg P(x)$ est vrai. Il s'ensuit que $\neg \forall x P(x)$ et $\exists x \neg P(x)$ sont logiquement équivalents.

Supposons que nous souhaitons annuler une quantification existentielle. Par exemple, considérez la proposition «Il y a un élève de cette classe qui a suivi un cours de calcul.» Ceci est l'existence quantification

$\exists x Q(x)$,

où $Q(x)$ est l'énoncé « x a suivi un cours de calcul». La négation de cet énoncé est la proposition «Ce n'est pas le cas qu'il y ait un étudiant dans cette classe qui a suivi un cours en calcul. "Cela équivaut à" Chaque élève de cette classe n'a pas pris le calcul ", ce qui est juste la quantification universelle de la négation de la fonction propositionnelle d'origine, ou, exprimée en le langage des quantificateurs,

$\forall x \neg Q(x)$.

Cet exemple illustre l'équivalence

$$\neg \exists x Q(x) \equiv \forall x \neg Q(x).$$

Pour montrer que $\neg \exists x Q(x)$ et $\forall x \neg Q(x)$ sont logiquement équivalents, peu importe ce qu'est $Q(x)$ et ce le domaine est, notons d'abord que $\neg \exists x Q(x)$ est vrai si et seulement si $\exists x Q(x)$ est faux. Cela est vrai si et

TABLEAU 2 **Lois de De Morgan pour les quantificateurs.**

Négation	*Déclaration équivalente*	*Quand la négation est-elle vraie?*	*Quand est-ce faux?*
$\neg \exists x P(x)$	$\forall x \neg P(x)$	Pour chaque x, $P(x)$ est faux.	Il y a un x pour lequel $P(x)$ est vrai.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	Il y a un x pour lequel $P(x)$ est faux.	$P(x)$ est vrai pour chaque x.

uniquement si aucun x n'existe dans le domaine pour lequel $Q(x)$ est vrai. Ensuite, notez qu'aucun x n'existe dans le domaine pour lequel $Q(x)$ est vrai si et seulement si $Q(x)$ est faux pour chaque x du domaine. Enfin, notez que $Q(x)$ est faux pour chaque x du domaine si et seulement si $\neg Q(x)$ est vrai pour tous les x du domaine, ce qui est vrai si et seulement si $\forall x \neg Q(x)$ est vrai. En rassemblant ces étapes, nous voyons que $\neg \exists x Q(x)$ est vrai si et seulement si $\forall x \neg Q(x)$ est vrai. Nous concluons que $\neg \exists x Q(x)$ et $\forall x \neg Q(x)$ sont logiquement équivalent.

Les règles de négation pour les quantificateurs sont appelées **lois de De Morgan pour les quantificateurs**. Celles-ci les règles sont résumées dans le tableau 2.

Remarque: Lorsque le domaine d'un prédicat $P(x)$ est composé de n éléments, où n est un positif entier supérieur à un, les règles de négation des instructions quantifiées sont exactement les mêmes que Les lois de De Morgan discutées dans la section 1.3. C'est pourquoi ces règles sont appelées De Morgan lois pour les quantificateurs. Lorsque le domaine a n éléments $x_1, x_2, \ldots, x_n$, il s'ensuit que $\neg \forall x P(x)$ est identique à $\neg(P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n))$, ce qui équivaut à $\neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n)$ par les lois de De Morgan, et c'est la même chose que $\exists x \neg P(x)$. De même, $\neg \exists x P(x)$

est identique à $\neg(P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n))$, qui selon les lois de De Morgan équivaut à
$\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \wedge \neg P(x_n)$, et c'est la même chose que $\forall x \neg P(x)$.

Nous illustrons la négation des énoncés quantifiés dans les exemples 20 et 21.

EXEMPLE 20 Quelles sont les négations des déclarations «Il y a un politicien honnête» et «Tous les Américains mangent cheeseburgers »?

Solution: Soit $H(x)$ dénoter « x est honnête». Puis la déclaration «Il y a un politicien honnête» est représenté par $\exists x H(x)$, où le domaine se compose de tous les politiciens.La négation de cette est $\neg\exists x H(x)$, ce qui équivaut à $\forall x \neg H(x)$. Cette négation peut être exprimée comme «Tout politicien est malhonnête.» (*Remarque:* en anglais, la déclaration «Tous les politiciens ne sont pas honnêtes» c'est ambigu. Dans l'usage courant, cette déclaration signifie souvent «Tous les politiciens ne sont pas honnêtes». Par conséquent, nous n'utilisons pas cette déclaration pour exprimer cette négation.)

Soit $C(x)$ « X mange des cheeseburgers». Ensuite, la déclaration «Tous les Américains mangent du fromage - hamburgers »est représenté par $\forall x C(x)$, où le domaine est composé de tous les Américains.La négation de cette déclaration est $\neg\forall x C(x)$, ce qui équivaut à $\exists x \neg C(x)$. Cette négation peut s'exprimer de plusieurs façons différentes, y compris "Certains Américains ne mangent pas de cheeseburgers" et "Il est un Américain qui ne mange pas de cheeseburgers. " ▲

EXEMPLE 21 Quelles sont les négations des énoncés $\forall x (x^2 > x)$ et $\exists x (x^2 = 2)$?

Solution: la négation de $\forall x (x^2 > x)$ est la déclaration $\neg\forall x (x^2 > x)$, qui équivaut à $\exists x \neg (x^2 > x)$. Cela peut être réécrit comme $\exists x (x^2 \leq x)$. La négation de $\exists x (x^2 = 2)$ est l'énoncé $\neg\exists x (x^2 = 2)$, ce qui équivaut à $\forall x \neg (x^2 = 2)$. Cela peut être réécrit comme $\forall x (x^2 \neq 2)$. le les valeurs de vérité de ces déclarations dépendent du domaine. ▲

Nous utilisons les lois de De Morgan pour les quantificateurs dans l'exemple 22.

EXEMPLE 22 Montrer que $\neg\forall x (P(x) \rightarrow Q(x))$ et $\exists x (P(x) \wedge \neg Q(x))$ sont logiquement équivalents.

Solution: Par la loi de De Morgan pour les quantificateurs universels, nous savons que $\neg\forall x (P(x) \rightarrow Q(x))$ et $\exists x (\neg(P(x) \rightarrow Q(x)))$ sont logiquement équivalents. Par la cinquième équivalence logique du tableau 7 dans la section 1.3, nous savons que $\neg(P(x) \rightarrow Q(x))$ et $P(x) \wedge \neg Q(x)$ sont logiquement équivalents pour chaque x . Parce que nous pouvons remplacer une expression logiquement équivalente par une autre dans un l'équivalence logique, il s'ensuit que $\neg\forall x (P(x) \rightarrow Q(x))$ et $\exists x (P(x) \wedge \neg Q(x))$ sont logiquement équivalent. ▲

Traduction de l'anglais en expressions logiques

La traduction de phrases en anglais (ou dans d'autres langues naturelles) en expressions logiques est un élément crucial tâche en mathématiques, programmation logique, intelligence artificielle, génie logiciel, et bien d'autres d'autres disciplines. Nous avons commencé à étudier ce sujet dans la section 1.1, où nous avons utilisé des propositions pour exprimer des phrases en expressions logiques. Dans cette discussion, nous avons délibérément évité les phrases dont les traductions nécessitaient des prédicats et des quantificateurs.Traduction de l'anglais vers un exemple logique les pressions deviennent encore plus complexes lorsque des quantificateurs sont nécessaires. De plus, il peut y avoir plusieurs façons de traduire une phrase particulière. (En conséquence, il n'y a pas de «livre de cuisine» approche qui peut être suivie étape par étape.) Nous utiliserons quelques exemples pour illustrer comment traduire des phrases de l'anglais en expressions logiques. Le but de cette traduction est de des expressions logiques simples et utiles. Dans cette section, nous nous limitons aux phrases qui peut être traduit en expressions logiques à l'aide d'un seul quantificateur; dans la section suivante, nous examinera des phrases plus compliquées qui nécessitent plusieurs quantificateurs.

EXEMPLE 23 Exprimer l'énoncé «Chaque élève de cette classe a étudié le calcul» à l'aide de prédicats et quantificateurs.

Solution: Tout d'abord, nous réécrivons l'énoncé afin d'identifier clairement les quantificateurs appropriés utiliser. Ce faisant, nous obtenons:

"Pour chaque élève de cette classe, cet élève a étudié le calcul."

Ensuite, nous introduisons une variable x pour que notre déclaration devienne

"Pour chaque élève x de cette classe, x a étudié le calcul."

Poursuivant, nous introduisons $C(x)$, qui est l'énoncé « x a étudié le calcul». Par conséquent, si le domaine pour x *se* compose des élèves de la classe, nous pouvons traduire notre déclaration par $\forall x C(x)$.

Cependant, il existe d'autres approches correctes; différents domaines du discours et autres des prédicats peuvent être utilisés. L'approche que nous choisissons dépend du raisonnement ultérieur que nous voulons réaliser. Par exemple, nous pouvons être intéressés par un groupe de personnes plus large que cette classe. Si nous changeons le domaine pour qu'il soit composé de toutes les personnes, nous devrons exprimer notre déclaration comme

"Pour chaque personne x , si la personne x est étudiante dans cette classe, alors x a étudié le calcul."

Si $S(x)$ représente l'affirmation selon laquelle la personne x est dans cette classe, nous voyons que notre affirmation peut être exprimée par $\forall x (S(x) \rightarrow C(x))$. [*Attention!* Notre déclaration *ne peut pas* être exprimée par $\forall x (S(x) \wedge C(x))$ parce que cette déclaration dit que toutes les personnes sont des étudiants de cette classe et ont étudié calcul!]

Enfin, lorsque nous nous intéressons à l'arrière-plan des personnes dans des sujets autres que le calcul, nous pouvons préférer utiliser le quantificateur à deux variables $Q(x, y)$ pour l'énoncé «l'élève x a étudié le sujet y . »Ensuite, nous remplacerions $C(x)$ par $Q(x,$ calcul) dans les deux approches pour obtenir $\forall x Q(x,$ calcul) ou $\forall x (S(x) \rightarrow Q(x,$ calcul)). ▲

Dans l'exemple 23, nous avons montré différentes approches pour exprimer la même déclaration en utilisant prédicats et quantificateurs. Cependant, nous devons toujours adopter l'approche la plus simple qui soit adéquat pour une utilisation dans le raisonnement ultérieur.

EXEMPLE 24 Exprimez les déclarations «Un élève de cette classe a visité le Mexique» et «Chaque élève cette classe a visité le Canada ou le Mexique »à l'aide de prédicats et de quantificateurs.

Solution: L'énoncé «Un élève de cette classe a visité le Mexique» signifie que

"Il y a un étudiant dans cette classe avec la propriété que l'étudiant a visité le Mexique."

Nous pouvons introduire une variable x , de sorte que notre déclaration devienne

"Il y a un étudiant x dans cette classe qui a la propriété que x a visité le Mexique."

Nous introduisons $M(x)$, qui est la déclaration «x a visité le Mexique». Si le domaine de x consiste des élèves de cette classe, nous pouvons traduire cette première affirmation par $\exists x M(x)$.

Cependant, si nous sommes intéressés par des personnes autres que celles de cette classe, nous regardons la déclaration un peu différemment. Notre déclaration peut être exprimée comme

«Il y a une personne x ayant les propriétés que x est un étudiant de cette classe et x a visité Mexique."

Dans ce cas, le domaine de la variable x comprend toutes les personnes. Nous introduisons $S(x)$ pour représenter « X est un élève de cette classe.» Notre solution devient $\exists x (S(x) \wedge M(x))$ parce que l'énoncé est qu'il y a une personne x qui est étudiante dans cette classe et qui a visité le Mexique. [*Attention!* Notre ne peut pas être exprimée par $\exists x (S(x) \rightarrow M(x))$, ce qui est vrai quand il n'y a pas quelqu'un dans la classe parce que, dans ce cas, pour une telle personne x , $S(x) \rightarrow M(x)$ devient soit $\mathbf{F} \rightarrow \mathbf{T}$ soit $\mathbf{F} \rightarrow \mathbf{F}$, les deux étant vrais.]

De même, la deuxième déclaration peut être exprimée comme suit:

"Pour chaque x de cette classe, x a la propriété que x a visité le Mexique ou x a visité Canada."

(Notez que nous supposons l'inclusif, plutôt que l'exclusif, ou ici.) Nous laissons $C(x)$ être « x a visité le Canada. »Suivant notre raisonnement précédent, nous voyons que si le domaine de x *se* compose de les élèves de cette classe, cette deuxième affirmation peut être exprimée par $\forall x (C(x) \vee M(x))$. cependant, si le domaine pour x *se* compose de toutes les personnes, notre déclaration peut être exprimée comme

«Pour chaque personne x , si x est un élève de cette classe, alors x a visité le Mexique ou x a visité Canada."

Dans ce cas, l'énoncé peut être exprimé par $\forall x (S(x) \rightarrow (C(x) \vee M(x)))$.

Au lieu d'utiliser $M(x)$ et $C(x)$ pour représenter que x a visité le Mexique et x a visité Au Canada, respectivement, nous pourrions utiliser un prédicat à deux positions $V(x, y)$ pour représenter « x a visité pays y . »Dans ce cas, $V(x,$ Mexique) et $V(x,$ Canada) auraient la même signification que $M(x)$ et $C(x)$ et pourrait les remplacer dans nos réponses. Si nous travaillons avec de nombreuses déclarations impliquer des personnes visitant différents pays, nous pourrions préférer utiliser cette approche à deux variables. Sinon, pour plus de simplicité, nous nous en tiendrons aux prédicats à une variable $M(x)$ et $C(x)$. ▲

Utilisation de quantificateurs dans les spécifications du système

Dans la section 1.2, nous avons utilisé des propositions pour représenter les spécifications du système.Cependant, de nombreux systèmes les spécifications impliquent des prédicats et des quantifications.Ceci est illustré dans l'exemple 25.

EXEMPLE 25 Utilisez des prédicats et des quantificateurs pour exprimer les spécifications du système «Chaque message électronique est plus grand plus d'un mégaoctet seront compressés "et" Si un utilisateur est actif, au moins une liaison réseau sera être disponible."

Solution: Soit $S(m, y)$ «le message électronique m est plus grand que y mégaoctets», où la variable x a le domaine de tous les messages électroniques et la variable y est un nombre réel positif, et que $C(m)$ désigne "Le message électronique m sera compressé." Ensuite, la spécification "Chaque message électronique supérieur à un mégaoctet sera compressé »peut être représenté par $\forall m (S(m, 1) \rightarrow C(m))$.

Rappelez-vous les règles de priorité pour les quantificateurs et des connecteurs logiques!

Soit $A(u)$ représente "L'utilisateur u est actif", où la variable u a le domaine de tous les utilisateurs, soit $S(n, x)$ dénote «La liaison réseau n est dans l'état x », où n a le domaine de tout le réseau links et x a le domaine de tous les états possibles pour une liaison réseau.Ensuite, la spécifica- «Si un utilisateur est actif, au moins une liaison réseau sera disponible» peut être représentée par $\exists u A(u) \rightarrow \exists n S(n,$ disponible$)$. ▲

Exemples de Lewis Carroll

Lewis Carroll (vraiment CL Dodgson écrit sous un pseudonyme), l'auteur d'*Alice in Wonder- terre* , est également l'auteur de plusieurs ouvrages sur la logique symbolique.Ses livres contiennent de nombreux exemples de raisonnement à l'aide de quantificateurs. Les exemples 26 et 27 proviennent de son livre *Symbolic Logic;* autre des exemples de ce livre sont donnés dans les exercices à la fin de cette section.Ces exemples illustrent comment les quantificateurs sont utilisés pour exprimer différents types de déclarations.

EXEMPLE 26 Tenez compte de ces déclarations. Les deux premiers sont appelés *locaux* et le troisième est appelé *conclusion* . L'ensemble est appelé un *argument* .

"Tous les lions sont féroces."
"Certains lions ne boivent pas de café."
"Certaines créatures féroces ne boivent pas de café."

(Dans la section 1.6, nous aborderons la question de savoir si la conclusion est une conséquence valable séquence des locaux. Dans cet exemple, c'est le cas.) Soit $P(x)$, $Q(x)$ et $R(x)$ les énoncés « x est un lion »,« x est féroce »et« x boit du café », respectivement. En supposant que le domaine se compose de tous créatures, exprimez les déclarations dans l'argument en utilisant des quantificateurs et $P(x)$, $Q(x)$ et $R(x)$.

CHARLES LUTWIDGE DODGSON (1832–1898) Nous connaissons Charles Dodgson sous le nom de Lewis Carroll — le pseudonyme qu'il a utilisé dans ses œuvres littéraires. Dodgson, le fils d'un ecclésiastique, était le troisième de 11 enfants, tous bégayaient. Il était mal à l'aise en compagnie d'adultes et aurait parlé sans bégayant seulement les jeunes filles, dont beaucoup il divertissait, correspondait et photographiait (parfois dans des poses qui seraient aujourd'hui jugées inappropriées). Bien qu'attiré par les jeunes filles, il était extrêmement puritains et religieux. Son amitié avec les trois jeunes filles de Dean Liddell l'a conduit à écrire *Alice au pays des merveilles* , ce qui lui a valu de l'argent et de la gloire.

Dodgson est diplômé d'Oxford en 1854 et a obtenu sa maîtrise ès arts en 1857. Il a été nommé professeur de mathématiques au Christ Church College, Oxford, en 1855. Il a été ordonné à l'Église d'Angleterre en 1861 mais n'a jamais exercé son ministère. Ses écrits publiés sous ce vrai nom comprennent des articles et des livres sur la géométrie, les déterminants et les mathématiques des tournois et des élections. (Il a également utilisé le pseudonyme Lewis Carroll pour ses nombreuses œuvres sur la logique récréative.)

Solution: Nous pouvons exprimer ces déclarations comme:

$\forall x\ (P\ (x) \rightarrow Q\ (x))$.
$\exists x\ (P\ (x) \wedge \neg R\ (x))$.
$\exists x\ (Q\ (x) \wedge \neg R\ (x))$.

Notez que la deuxième instruction ne peut pas être écrite comme $\exists x\ (P\ (x) \rightarrow \neg R\ (x))$. La raison en est que $P\ (x) \rightarrow \neg R\ (x)$ est vrai chaque fois que x n'est pas un lion, de sorte que $\exists x\ (P\ (x) \rightarrow \neg R\ (x))$ est vrai tant que il y a au moins une créature qui n'est pas un lion, même si chaque lion boit du café.De même, le la troisième déclaration ne peut pas être écrite comme

$\exists x\ (Q\ (x) \rightarrow \neg R\ (x))$. ▲

EXEMPLE 27 Considérez ces déclarations, dont les trois premières sont des prémisses et la quatrième est une conclusion valable. sion.

"Tous les colibris sont richement colorés."
"Aucun gros oiseau ne vit de miel."
"Les oiseaux qui ne vivent pas de miel sont de couleur terne."
"Les colibris sont petits."

Soit $P\ (x)$, $Q\ (x)$, $R\ (x)$ et $S\ (x)$ les énoncés « x est un colibri», « x est grand», « x vit miel »et« x est richement coloré », respectivement.En supposant que le domaine se compose de tous les oiseaux, exprimer les déclarations dans l'argument en utilisant des quantificateurs et $P\ (x)$, $Q\ (x)$, $R\ (x)$ et $S\ (x)$.

Solution: Nous pouvons exprimer les déclarations dans l'argument comme

$\forall x\ (P\ (x) \rightarrow S\ (x))$.
$\neg\exists x\ (Q\ (x) \wedge R\ (x))$.
$\forall x\ (\neg R\ (x) \rightarrow \neg S\ (x))$.
$\forall x\ (P\ (x) \rightarrow \neg Q\ (x))$.

(Notez que nous avons supposé que «petit» est le même que «pas grand» et que «de couleur terne» est le comme «pas richement coloré». Pour montrer que la quatrième déclaration est une conclusion valable de la première troisièmement, nous devons utiliser des règles d'inférence qui seront discutées dans la section 1.6.) ▲

Programmation logique

Un type important de langage de programmation est conçu pour raisonner en utilisant les règles de prédicat logique. Prolog (de *Pro* gramming in *Log* ic), développé dans les années 1970 par des informaticiens travaillant dans le domaine de l'intelligence artificielle, est un exemple d'un tel langage. Programmes Prolog comprennent un ensemble de déclarations comprenant deux types de déclarations, les **faits Prolog** et **Prolog règles** . Les faits Prolog définissent les prédicats en spécifiant les éléments qui satisfont ces prédicats. Les règles Prolog sont utilisées pour définir de nouveaux prédicats en utilisant ceux déjà définis par les faits Prolog. L'exemple 28 illustre ces notions.

EXEMPLE 28 Envisager un programme Prolog compte tenu des faits lui indiquant l'instructeur de chaque classe et dans quelles classes les étudiants sont inscrits. Le programme utilise ces faits pour répondre aux questions concernant les professeurs qui enseignent à des étudiants particuliers. Un tel programme pourrait utiliser l' *instructeur de* prédicats *(p, c)* et *inscrit (s, c)* pour représenter que le professeur p est l'instructeur du cours c et que l'élève s est inscrit au cours c, respectivement. Par exemple, les faits Prolog dans un tel programme peuvent comprendre:

```
instructeur (chan, math273)
instructeur (patel, ee222)
instructeur (grossman, cs301)
inscrit (kevin, math273)
inscrits (juana, ee222)
inscrit (juana, cs301)
inscrit (kiko, math273)
inscrit (kiko, cs301)
```

(Des lettres minuscules ont été utilisées pour les entrées car Prolog considère les noms commençant par une lettre majuscule pour être des variables.)

Un nouveau prédicat *enseigne (p, s)*, ce qui représente que le professeur p enseigne étudiant s, peut être défini à l'aide de la règle Prolog

```
enseigne (P, S): - instructeur (P, C), inscrit (S, C)
```

ce qui signifie que *enseigne (p, s)* est vrai s'il existe une classe c telle que le professeur p est le l'instructeur de classe c et l'élève s sont inscrits en classe c. (Notez qu'une virgule est utilisée pour représenter une conjonction de prédicats dans Prolog. De même, un point-virgule est utilisé pour représenter une disjonction de prédicats.)

Prolog répond aux requêtes en utilisant les faits et les règles qui lui sont donnés.Par exemple, en utilisant les faits et les règles répertoriées, la requête

```
? inscrit (kevin, math273)
```

produit la réponse

```
Oui
```

parce que le fait *inscrit* (kevin, math273) a été fourni en entrée. La requête

```
? inscrit (X, math273)
```

produit la réponse

```
Kevin
kiko
```

Pour produire cette réponse, Prolog détermine toutes les valeurs possibles de X pour lesquelles *inscrit* (X, math273) a été inclus comme fait Prolog.De même, pour trouver tous les professeurs qui sont instructeurs dans les cours suivis par Juana, nous utilisons la requête

```
? enseigne (X, juana)
```

Cette requête renvoie

```
patel
homme dégoutant
```

Des exercices

1. Soit $P(x)$ la phrase « $x \leq 4$.» Que sont ces valeurs de vérité?

a) $P(0)$ **b)** $P(4)$ **c)** $P(6)$

2. Soit $P(x)$ l'énoncé «le mot x contient le lettre a . »Quelles sont ces valeurs de vérité?

a) P (orange) **b)** P (citron)
c) P (vrai) **d)** P (faux)

3. Soit $Q(x, y)$ la phrase « x est la capitale de y ». Quelles sont ces valeurs de vérité?

a) Q (Denver, Colorado)
b) Q (Détroit, Michigan)
c) Q (Massachusetts, Boston)
d) Q (New York, New York)

4. Indiquez la valeur de x après l'instruction **si** $P(x)$ **alors** $x := 1$ est exécuté, où $P(x)$ est la déclaration « $x > 1$», si le la valeur de x lorsque cette instruction est atteinte est

a) $x = 0$. **b)** $x = 1$.
c) $x = 2$.

5. Soit $P(x)$ l'énoncé « x passe plus de cinq heures chaque jour de la semaine en classe ", où le domaine pour x *se* compose de tous les étudiants. Exprimez chacune de ces quantifications en Anglais.

a) $\exists xP(x)$ **b)** $\forall xP(x)$
c) $\exists x \neg P(x)$ **d)** $\forall x \neg P(x)$

6. Soit $N(x)$ la déclaration « x a visité le Dakota du Nord» où le domaine se compose des élèves de votre école. Exprimez chacune de ces quantifications en anglais.

a) $\exists xN(x)$ **b)** $\forall xN(x)$ **c)** $\neg\exists xN(x)$
d) $\exists x \neg N(x)$ **e)** $\neg\forall xN(x)$ **f)** $\forall x \neg N(x)$

7. Traduisez ces déclarations en anglais, où $C(x)$ est « x est un comédien "et $F(x)$ est" x est drôle "et le domaine se compose de toutes les personnes.

a) $\forall x (C(x) \rightarrow F(x))$ **b)** $\forall x (C(x) \wedge F(x))$
c) $\exists x (C(x) \rightarrow F(x))$ **d)** $\exists x (C(x) \wedge F(x))$

8. Traduisez ces déclarations en anglais, où $R(x)$ est « x est un lapin "et $H(x)$ est" x houblon "et le domaine se compose de tous les animaux.

a) $\forall x (R(x) \rightarrow H(x))$ **b)** $\forall x (R(x) \wedge H(x))$
c) $\exists x (R(x) \rightarrow H(x))$ **d)** $\exists x (R(x) \wedge H(x))$

9. Soit $P(x)$ la déclaration « x peut parler russe» et laisse $Q(x)$ être l'énoncé « x connaît le langage informatique C ++. "Exprimez chacune de ces phrases en termes de $P(x)$, $Q(x)$, quantificateurs et connecteurs logiques. Le domaine pour les quantificateurs se compose de tous les élèves de votre école.

a) Un élève de votre école peut parler le russe sian et qui connaît le C ++.
b) Un élève de votre école peut parler le russe sian mais qui ne connaît pas le C ++.
c) Chaque élève de votre école peut parler russe ou connaît C ++.
d) Aucun élève de votre école ne peut parler russe ou ne sait C ++.

10. Soit $C(x)$ l'énoncé « x a un chat», soit $D(x)$ le déclaration « x a un chien», et soit $F(x)$ la déclaration « x a un furet. "Exprimez chacune de ces déclarations en termes de $C(x)$, $D(x)$, $F(x)$, quantificateurs et connecteurs logiques. Laissez le domaine se composer de tous les élèves de votre classe.

a) Un élève de votre classe a un chat, un chien et un furet.
b) Tous les élèves de votre classe ont un chat, un chien ou un furet.
c) Un élève de votre classe a un chat et un furet, mais pas un chien.
d) Aucun élève de votre classe n'a de chat, de chien et de furet.
e) Pour chacun des trois animaux, chats, chiens et furets, il y a un élève dans votre classe qui a cet animal comme un animal de compagnie.

11. Soit $P(x)$ l'énoncé « $x = x^2$ ». Si le domaine consistes des entiers, quelles sont ces valeurs de vérité?

a) $P(0)$ **b)** $P(1)$ **c)** $P(2)$
d) $P(-1)$ **e)** $\exists xP(x)$ **f)** $\forall xP(x)$

12. Soit $Q(x)$ l'énoncé « $x + 1 > 2x$ ». Si le domaine se compose de tous les entiers, quelles sont ces valeurs de vérité?

a) $Q(0)$ **b)** $Q(-1)$ **c)** $Q(1)$
d) $\exists xQ(x)$ **e)** $\forall xQ(x)$ **f)** $\exists x \neg Q(x)$
g) $\forall x \neg Q(x)$

13. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine se compose de tous les entiers.

a) $\forall n (n + 1 > n)$ **b)** $\exists n (2n = 3n)$
c) $\exists n (n = -n)$ **d)** $\forall n (3n \leq 4n)$

14. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine se compose de tous les nombres réels.

a) $\exists x (x^3 = -1)$ **b)** $\exists x (x^4 < x^2)$
c) $\forall x ((-x)^2 = x^2)$ **d)** $\forall x (2x > x)$

15. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine pour toutes les variables se compose de tous les entiers.

a) $\forall n (n^2 \geq 0)$ **b)** $\exists n (n^2 = 2)$
c) $\forall n (n^2 \geq n)$ **d)** $\exists n (n^2 < 0)$

16. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine de chaque variable est constitué de tous les nombres réels.

a) $\exists x (x^2 = 2)$ **b)** $\exists x (x^2 = -1)$
c) $\forall x (x^2 + 2 \geq 1)$ **d)** $\forall x (x^2 = x)$

17. Supposons que le domaine de la fonction propositionnelle $P(x)$ *se* compose des entiers 0, 1, 2, 3 et 4. Écrivez chacune de ces propositions en utilisant des disjonctions, et négations.

a) $\exists xP(x)$ **b)** $\forall xP(x)$ **c)** $\exists x \neg P(x)$
d) $\forall x \neg P(x)$ **e)** $\neg\exists xP(x)$ **f)** $\neg\forall xP(x)$

18. Supposons que le domaine de la fonction propositionnelle $P(x)$ *se* compose des nombres entiers -2, -1, 0, 1 et 2. Écriture chacune de ces propositions en utilisant des disjonctions, jonctions et négations.

a) $\exists xP(x)$ **b)** $\forall xP(x)$ **c)** $\exists x \neg P(x)$
d) $\forall x \neg P(x)$ **e)** $\neg\exists xP(x)$ **f)** $\neg\forall xP(x)$

19. Supposons que le domaine de la fonction propositionnelle $P(x)$ *se* compose des entiers 1, 2, 3, 4 et 5. Express ces déclarations sans utiliser de quantificateurs, à la place en utilisant seules les négations, les disjonctions et les conjonctions.

a) $\exists xP(x)$ **b)** $\forall xP(x)$
c) $\neg\exists xP(x)$ **d)** $\neg\forall xP(x)$
e) $\forall x ((x = 3) \rightarrow P(x)) \vee \exists x \neg P(x)$

20. Supposons que le domaine de la fonction propositionnelle $P(x)$ *se* compose de −5, −3, −1, 1, 3 et 5. Exprimez-les sans utiliser de quantificateurs, au lieu d'utiliser uniquement

e) Tout le monde est votre ami et est parfait.
f) Tout le monde n'est pas votre ami ou quelqu'un n'est pas perfect.

26. Traduire chacune de ces déclarations en expressions logiques sions de trois manières différentes en variant le domaine et en utilisant des prédicats avec une et deux variables.

a) Un membre de votre école s'est rendu en Ouzbékistan.
b) Tout le monde dans votre classe a étudié le calcul et le C ++.
c) Personne dans votre école ne possède à la fois un vélo et un

négations, disjonctions et conjonctions.

a) $\exists xP(x)$ **b)** $\forall xP(x)$
c) $\forall x((x=1) \rightarrow P(x))$
d) $\exists x((x \geq 0) \wedge P(x))$
e) $\exists x(\neg P(x)) \wedge \forall x((x<0) \rightarrow P(x))$

21. Pour chacune de ces déclarations, trouvez un domaine pour lequel l'instruction est vraie et un domaine pour lequel l'instruction est faux.

a) Tout le monde étudie les mathématiques discrètes.
b) Tout le monde a plus de 21 ans.
c) Toutes les deux personnes ont la même mère.
d) Deux personnes différentes n'ont pas la même grand-mère.

22. Pour chacune de ces déclarations, trouvez un domaine pour lequel l'instruction est vraie et un domaine pour lequel l'instruction est faux.

a) Tout le monde parle hindi.
b) Il y a quelqu'un de plus de 21 ans.
c) Toutes les deux personnes ont le même prénom.
d) Quelqu'un connaît plus de deux autres personnes.

23. Traduisez de deux manières chacune de ces déclarations en expressions cal à l'aide de prédicats, de quantificateurs et de logiques connecteurs. Tout d'abord, laissez le domaine se composer des étudiants dans votre classe et ensuite, laissez-le se composer de tous les gens.

a) Quelqu'un dans votre classe peut parler l'hindi.
b) Tout le monde dans votre classe est amical.
c) Il y a une personne dans votre classe qui n'est pas née en Californie.
d) Un élève de votre classe a été dans un film.
e) Aucun élève de votre classe n'a suivi un cours de logique programmation.

24. Traduisez de deux manières chacune de ces déclarations en expressions cal à l'aide de prédicats, de quantificateurs et de logiques connecteurs. Tout d'abord, laissez le domaine se composer des étudiants dans votre classe et ensuite, laissez-le se composer de tous les gens.

a) Tout le monde dans votre classe a un téléphone cellulaire.
b) Quelqu'un de ta classe a vu un film étranger.
c) Il y a une personne dans votre classe qui ne sait pas nager.
d) Tous les élèves de votre classe peuvent résoudre des équations quadratiques tions.
e) Certains élèves de votre classe ne veulent pas être riches.

25. Traduisez chacune de ces déclarations en expressions logiques utilisant des prédicats, des quantificateurs et des connexions logiques tives.

a) Personne n'est parfait.
b) Tout le monde n'est pas parfait.
c) Tous vos amis sont parfaits.
d) Au moins un de vos amis est parfait.

moto.

d) Il y a une personne dans ton école qui n'est pas heureuse.

e) Tout le monde dans votre école est né dans le vingtième siècle.

27. Traduire chacune de ces déclarations en expressions logiques sions de trois manières différentes en variant le domaine et en utilisant des prédicats avec une et deux variables.

a) Un élève de votre école a vécu au Vietnam.

b) Il y a un élève dans votre école qui ne peut pas parler Hindi.

c) Un élève de votre école connaît Java, Prolog et C ++.

d) Tout le monde dans votre classe aime la cuisine thaïlandaise.

e) Un membre de votre classe ne joue pas au hockey.

28. Traduire chacune de ces déclarations en expressions logiques utilisant des prédicats, des quantificateurs et des connexions logiques tives.

a) Quelque chose n'est pas au bon endroit.

b) Tous les outils sont au bon endroit et sont en excellent état état.

c) Tout est au bon endroit et en excellent état édition.

d) Rien n'est au bon endroit et est en excellent état édition.

e) Un de vos outils n'est pas au bon endroit, mais il est En excellent état.

29. Exprimez chacune de ces déclarations à l'aide d'opérateurs logiques, prédicats et quantificateurs.

a) Certaines propositions sont des tautologies.

b) La négation d'une contradiction est une tautologie.

c) La disjonction de deux contingences peut être une tautol-ogy.

d) La conjonction de deux tautologies est une tautologie.

30. Supposons le domaine de la fonction propositionnelle $P(x, y)$ se compose des paires x et y , où x est 1, 2 ou 3 et y est 1, 2 ou 3. Écrivez ces propositions en utilisant des disjonctions et les conjonctions.

a) $\exists x P(x, 3)$ **b)** $\forall yP(1, y)$
c) $\exists y \neg P(2, y)$ **d)** $\forall x \neg P(x, 2)$

31. Supposons que le domaine de $Q(x, y, z)$ *se* compose de triplets x, y, z , où $x = 0$, 1 , ou 2, $y = 0$ ou 1, et $z = 0$ ou 1.

Écrivez ces propositions en utilisant des disjonctions et jonctions.

a) $\forall yQ(0, y, 0)$ **b)** $\exists xQ(x, 1, 1)$
c) $\exists z \neg Q(0, 0, z)$ **d)** $\exists x \neg Q(x, 0, 1)$

32. Exprimez chacune de ces déclarations à l'aide de quantificateurs. alors former la négation de la déclaration afin qu'aucune négation ne soit à gauche d'un quantificateur. Ensuite, exprimez la négation dans anglais simple. (N'utilisez pas simplement l'expression «Ce n'est pas le cas. ")

a) Tous les chiens ont des puces.

b) Il y a un cheval qui peut ajouter.

c) Chaque koala peut grimper.

d) Aucun singe ne peut parler français.

e) Il existe un cochon qui peut nager et attraper des poissons.

33. Exprimez chacune de ces déclarations à l'aide de quantificateurs. alors former la négation de la déclaration, de sorte qu'aucune négation est à gauche d'un quantificateur. Ensuite, exprimez la négation dans anglais simple. (N'utilisez pas simplement l'expression «Ce n'est pas le cas. ")

a) Certains vieux chiens peuvent apprendre de nouveaux trucs.

b) Aucun lapin ne connaît le calcul.

c) Chaque oiseau peut voler.

d) Aucun chien ne peut parler.

e) Personne dans cette classe ne connaît le français et Russe.

34. Exprimer la négation de ces propositions en utilisant des fiers, puis exprimer la négation en anglais.

a) Certains conducteurs n'obéissent pas à la limite de vitesse.

Les exercices 38 à 42 traitent de la traduction entre les systèmes spécification et expressions logiques impliquant des quantificateurs.

38. Traduire ces spécifications système en anglais où le prédicat $S(x, y)$ est " x est dans l'état y " et où le domaine pour x et y *se* compose de tous les systèmes et tous les possibles États, respectivement.

a) $\exists xS(x,$ ouvert$)$

b) $\forall x(S(x,$ dysfonctionnement$) \vee S(x,$ diagnostic$))$

c) $\exists xS(x,$ ouvert$) \vee \exists xS(x,$ diagnostic$)$

d) $\exists x \neg S(x,$ disponible$)$

e) $\forall x \neg S(x,$ *en* fonctionnement$)$

39. Traduire ces spécifications en anglais où $F(p)$ est «L'imprimante p est hors service», $B(p)$ est «L'imprimante p est occupée» $L(j)$ est «Le travail d'impression j est perdu» et $Q(j)$ est «Le travail d'impression j est en file d'attente. "

a) $\exists p(F(p) \wedge B(p)) \rightarrow \exists jL(j)$

b) $\forall pB(p) \rightarrow \exists jQ(j)$

c) $\exists j(Q(j) \wedge L(j)) \rightarrow \exists pF(p)$

d) $(\forall pB(p) \wedge \forall jQ(j)) \rightarrow \exists jL(j)$

40. Exprimez chacune de ces spécifications de système en utilisant cates, quantificateurs et connecteurs logiques.

a) Lorsqu'il y a moins de 30 mégaoctets sur le disque dur

b) Tous les films suédois sont sérieux.

c) Personne ne peut garder un secret.

d) Il y a quelqu'un dans cette classe qui n'a pas de bonne attitude.

35. Trouver un contre-exemple, si possible, à ces universellement déclarations quantifiées, où le domaine pour toutes les variables se compose de tous les entiers.

a) $\forall x\ (x^2 \geq x)$

b) $\forall x\ (x > 0 \lor x < 0)$

c) $\forall x\ (x = 1)$

36. Trouver un contre-exemple, si possible, à ces universellement déclarations quantifiées, où le domaine pour toutes les variables se compose de tous les nombres réels.

a) $\forall x\ (x^2 = x)$ **b)** $\forall x\ (x^2 = 2)$

c) $\forall x\ (|x| > 0)$

37. Exprimez chacune de ces déclarations en utilisant des prédicats et quantificateurs.

a) Un passager d'une compagnie aérienne est considéré comme un voyageur d'élite si le passager vole plus de 25 000 milles en un an ou prend plus de 25 vols au cours de cette année.

b) Un homme se qualifie pour le marathon si sa meilleure temps est inférieur à 3 heures et une femme est éligible pour le marathon si son meilleur temps précédent est inférieur à 3,5 heures.

c) Un étudiant doit suivre au moins 60 heures de cours, ou au moins 45 heures de cours et rédiger une thèse de maîtrise, et recevoir une note non inférieure à B dans tous les cours obligatoires, pour recevoir une maîtrise.

d) Il y a un étudiant qui a pris plus de 21 crédits heures dans un semestre et a reçu tous les A.

disque, un message d'avertissement est envoyé à tous les utilisateurs.

b) Aucun répertoire du système de fichiers ne peut être ouvert et aucun fichier ne peut être fermé lorsque des erreurs système ont été détectées détectée.

c) Le système de fichiers ne peut pas être sauvegardé s'il y a un utilisateur actuellement connecté.

d) La vidéo à la demande peut être livrée lorsqu'il y a au moins 8 mégaoctets de mémoire disponible et la La vitesse de connexion est d'au moins 56 kilobits par seconde.

41. Exprimez chacune de ces spécifications de système en utilisant cates, quantificateurs et connecteurs logiques.

a) Au moins un message électronique, parmi l'ensemble non vide de messages, peut être enregistré s'il y a un disque avec plus de 10 kilo-octets d'espace libre.

b) Chaque fois qu'une alerte est active, tous les messages en file d'attente sont transmises.

c) Le moniteur de diagnostic suit l'état de tous les systèmes sauf la console principale.

d) Chaque participant à la conférence téléphonique que l'hôte de l'appel n'a pas mis sur une liste spéciale a été facturée.

42. Exprimez chacune de ces spécifications de système en utilisant cates, quantificateurs et connecteurs logiques.

a) Chaque utilisateur a accès à une boîte aux lettres électronique.

b) La boîte aux lettres système est accessible à tous le groupe si le système de fichiers est verrouillé.

c) Le pare-feu est dans un état de diagnostic uniquement si le proxy le serveur est dans un état de diagnostic.

d) Au moins un routeur fonctionne normalement si le le débit est compris entre 100 kbps et 500 kbps et le serveur proxy n'est pas en mode diagnostic.

43. Déterminez si $\forall x\ (P(x) \rightarrow Q(x))$ et $\forall x P(x) \rightarrow \forall x Q(x)$ sont logiquement équivalents. Justifiez votre réponse.

44. Déterminer si $\forall x\ (P(x) \leftrightarrow Q(x))$ et $\forall x\ P(x) \leftrightarrow \forall x Q(x)$ sont logiquement équivalents. Justifiez votre réponse.

45. Montrer que $\exists x\ (P(x) \lor Q(x))$ et $\exists x P(x) \lor \exists x Q(x)$ sont logiquement équivalent.

Les exercices 46 à 49 établissent des règles de **quantification nulle** qui nous pouvons utiliser lorsqu'une variable quantifiée n'apparaît pas en partie d'une déclaration.

46. Établir ces équivalences logiques, où x ne correspond pas produire comme une variable libre dans A . Supposons que le domaine est non vide.

a) $(\forall x P(x)) \lor A \equiv \forall x\ (P(x) \lor A)$

b) $(\exists x P(x)) \lor A \equiv \exists x\ (P(x) \lor A)$

47. Établir ces équivalences logiques, où x ne correspond pas produire comme une variable libre dans A . Supposons que le domaine est non vide.

a) $(\forall x P(x)) \land A \equiv \forall x\ (P(x) \land A)$

b) $(\exists x P(x)) \land A \equiv \exists x\ (P(x) \land A)$

48. Établir ces équivalences logiques, où x ne correspond pas produire comme une variable libre dans A . Supposons que le domaine est non vide.

a) $\forall x\ (A \rightarrow P(x)) \equiv A \rightarrow \forall x P(x)$

b) $\exists x\ (A \rightarrow P(x)) \equiv A \rightarrow \exists x P(x)$

49. Établir ces équivalences logiques, où x ne correspond pas produire comme une variable libre dans A . Supposons que le domaine est non vide.

a) $\forall x\ (P(x) \rightarrow A) \equiv \exists x P(x) \rightarrow A$

b) $\exists x\ (P(x) \rightarrow A) \equiv \forall x P(x) \rightarrow A$

50. Montrer que $\forall x P(x) \lor \forall x Q(x)$ et $\forall x\ (P(x) \lor Q(x))$ sont pas logiquement équivalent.

51. Montrer que $\exists x P(x) \land \exists x Q(x)$ et $\exists x\ (P(x) \land Q(x))$ sont pas logiquement équivalent.

52. Comme mentionné dans le texte, la notation $\exists! x P(x)$ désigne

"Il existe un x unique tel que $P(x)$ soit vrai."

Si le domaine est composé de tous les entiers, quelle est la vérité valeurs de ces déclarations?

56. Compte tenu des faits de Prolog dans l'exemple 28, que serait Prolog retourner lorsque ces requêtes sont données?

a) ? inscrit (kevin, ee222)

b) ? inscrit (kiko, math273)

c) ? instructeur (grossman, X)

d) ? instructeur (X, cs301)

e) ? enseigne (X, kevin)

57. Supposons que les faits Prolog soient utilisés pour définir les prédicats *mère (M, Y)* et *père (F, X)* , qui représentent que M est la mère de Y et F est le père de X , respectivement. Donnez une règle Prolog pour définir le *frère* prédicat *(X, Y)* , qui représente que X et Y sont frères et sœurs (c'est-à-dire, ont la même mère et le même père).

58. Supposons que les faits Prolog soient utilisés pour définir le la *mère (M, Y)* et le *père (F, X)* , qui représentent que M est la mère de Y et F est le père de X , respectivement. Donnez une règle Prolog pour définir le prédicat *grand-père (X, Y)* , qui représente que X est le grand-père de Y . [*Astuce:* vous pouvez écrire une disjonction dans Prolog soit en utilisant un point-virgule pour séparer les prédicats ou en mettre ces prédicats sur des lignes distinctes.]

Les exercices 59 à 62 sont basés sur des questions trouvées dans le livre *Logique symbolique* par Lewis Carroll.

59. Soit $P(x)$, $Q(x)$ et $R(x)$ les énoncés « x est un professeur »,« x est ignorant »et« x est vain », respectivement. Exprimez chacune de ces déclarations à l'aide de quantificateurs; Journal-connecteurs connectiques; et $P(x)$, $Q(x)$ et $R(x)$, où le Le domaine est composé de toutes les personnes.

a) Aucun professeur n'est ignorant.

b) Tous les ignorants sont vains.

c) Aucun professeur n'est vain.

d) Est-ce que (c) découle de (a) et (b)?

60. Soit $P(x)$, $Q(x)$ et $R(x)$ les énoncés « x est un clair explication "," x est satisfaisant "et" x est une excuse ", respectivement. Supposons que le domaine pour x *se* compose de tous Texte en anglais. Exprimez chacune de ces déclarations en utilisant tificateurs, connecteurs logiques et $P(x)$, $Q(x)$ et $R(x)$.

a) Toutes les explications claires sont satisfaisantes.

a) $\exists! x\,(x > 1)$ **b)** $\exists! x\,(x^2 = 1)$
c) $\exists! x\,(x + 3 = 2x)$ **d)** $\exists! x\,(x = x + 1)$

53. Quelles sont les valeurs de vérité de ces déclarations?

a) $\exists! xP(x) \rightarrow \exists xP(x)$

b) $\forall xP(x) \rightarrow \exists! xP(x)$

c) $\exists! x \neg P(x) \rightarrow \neg\forall xP(x)$

54. Écrivez $\exists! xP(x)$, où le domaine se compose de l'integers 1, 2 et 3, en termes de négations, de conjonctions, et les disjonctions.

55. Compte tenu des faits Prolog dans l'exemple 28, que serait Prolog retour étant donné ces requêtes?

a) ? instructeur (chan, math273)

b) ? instructeur (patel, cs301)

c) ? inscrit (X, cs301)

d) ? inscrit (kiko, Y)

e) ? enseigne (grossman, Y)

b) Certaines excuses ne sont pas satisfaisantes.

c) Certaines excuses ne sont pas des explications claires.

* **d)** (c) découle-t-il de (a) et (b)?

61. Soit $P(x)$, $Q(x)$, $R(x)$ et $S(x)$ les énoncés « x est un bébé »,« x est logique »,« x est capable de gérer un crocodile », et « x est méprisé», respectivement. Supposons que le domaine se compose de toutes les personnes. Exprimez chacune de ces déclarations en utilisant des quantificateurs; connecteurs logiques; et $P(x)$, $Q(x)$, $R(x)$ et $S(x)$.

a) Les bébés sont illogiques.

b) Personne n'est méprisé qui peut gérer un crocodile.

c) Les personnes illogiques sont méprisées.

d) Les bébés ne peuvent pas gérer les crocodiles.

* **e)** Est-ce que (d) découle de (a), (b) et (c)? Sinon, y a-t-il une conclusion correcte?

62. Soit $P(x)$, $Q(x)$, $R(x)$ et $S(x)$ les énoncés « x est un canard "," x est une de mes volailles "," x est un officier ", et « x est prêt à valser», respectivement. Exprimez chacun ces déclarations à l'aide de quantificateurs; connecteurs logiques; et $P(x)$, $Q(x)$, $R(x)$ et $S(x)$.

a) Aucun canard n'est prêt à valser.

b) Aucun officier ne refuse de valser.

c) Toutes mes volailles sont des canards.

d) Mes volailles ne sont pas des officiers.

* **e)** Est-ce que (d) découle de (a), (b) et (c)? Sinon, y a-t-il une conclusion correcte?

Quantificateurs imbriqués

introduction

Dans la section 1.4, nous avons défini les quantificateurs existentiels et universels et montré comment ils peuvent être utilisé pour représenter des énoncés mathématiques. Nous avons également expliqué comment ils peuvent être utilisés pour traduire des phrases anglaises en expressions logiques. Cependant, dans la section 1.4, nous avons évité l'**imbrication quantificateurs**, où un quantificateur est dans la portée d'un autre, tel que

$$\forall x \exists y\,(x + y = 0).$$

Notez que tout ce qui est dans le cadre d'un quantificateur peut être considéré comme une fonction propositionnelle. Par exemple,

$$\forall x \exists y\,(x + y = 0)$$

est la même chose que $\forall xQ(x)$, où $Q(x)$ est $\exists yP(x, y)$, où $P(x, y)$ est $x + y = 0$.

Les quantificateurs imbriqués se produisent couramment en mathématiques et en informatique. Bien imbriqué quantificateurs peuvent parfois être difficiles à comprendre, les règles que nous avons déjà étudiées dans La section 1.4 peut nous aider à les utiliser. Dans cette section, nous allons acquérir une expérience de travail avec quantificateurs. Nous verrons comment utiliser des quantificateurs imbriqués pour exprimer des énoncés mathématiques tels comme "La somme de deux entiers positifs est toujours positive." Nous allons montrer comment les quantificateurs imbriqués peut être utilisé pour traduire des phrases en anglais telles que «Tout le monde a exactement un meilleur ami» en déclarations logiques. De plus, nous acquerrons de l'expérience en travaillant avec les négations des déclarations impliquant des quantificateurs imbriqués.

Présentation des instructions impliquant des quantificateurs imbriqués

Pour comprendre les déclarations impliquant des quantificateurs imbriqués, nous devons découvrir ce que les quantificateurs et les prédicats qui semblent moyens. Ceci est illustré dans les exemples 1 et 2.

EXEMPLE 1 Supposons que le domaine des variables x et y *se* compose de tous les nombres réels. La déclaration

$$\forall x \forall y\,(x + y = y + x)$$

dit que $x + y = y + x$ pour tous les nombres réels x et y. Ceci est la loi commutative pour l'addition de nombres réels. De même, la déclaration

$$\forall x \exists y\,(x + y = 0)$$

dit que pour chaque nombre réel x, il existe un nombre réel y tel que $x + y = 0$. Cela indique que chaque nombre réel a un inverse additif. De même, la déclaration

$$\forall x \forall y \forall z\,(x + (y + z) = (x + y) + z)$$

est la loi associative pour l'addition de nombres réels. ▲

EXEMPLE 2 Traduire en anglais la déclaration

$$\forall x \forall y ((x > 0) \wedge (y < 0) \rightarrow (xy < 0)),$$

où le domaine pour les deux variables se compose de tous les nombres réels.

Solution: Cette déclaration dit que pour chaque nombre réel x et pour chaque nombre réel y, si $x > 0$ et $y < 0$, puis $xy < 0$. Autrement dit, cette déclaration dit que pour les nombres réels x et y, si x est positif et y est négatif, alors xy est négatif. Cela peut être dit plus succinctement comme «Le produit d'un un nombre réel positif et un nombre réel négatif est toujours un nombre réel négatif. » ▲

PENSER LA QUANTIFICATION COMME BOUCLES En travaillant avec des quantifications de plus d'une variable, il est parfois utile de penser en termes de boucles imbriquées.(Bien sûr, s'il y a sont infiniment nombreux éléments dans le domaine d'une variable, nous ne pouvons pas réellement parcourir toutes les valeurs. Néanmoins, cette façon de penser est utile pour comprendre les quantificateurs imbriqués.) Pour par exemple, pour voir si $\forall x \forall y P(x, y)$ est vrai, nous *parcourons* les valeurs de x et de chaque x nous parcourons les valeurs de y. Si nous constatons que $P(x, y)$ est vrai pour toutes les valeurs de x et y, nous ont déterminé que $\forall x \forall y P(x, y)$ est vrai. Si jamais nous atteignons une valeur x pour laquelle nous frappons une valeur y pour laquelle $P(x, y)$ est faux, nous avons montré que $\forall x \forall y P(x, y)$ est faux.

De même, pour déterminer si $\forall x \exists y P(x, y)$ est vrai, nous *parcourons* les valeurs de x. Pour chaque x, nous parcourons les valeurs de y jusqu'à ce que nous trouvions un y pour lequel $P(x, y)$ est vrai. Si pour chaque x nous *frappons* un tel y, alors $\forall x \exists y P(x, y)$ est vrai; si pour certains x nous ne frappons jamais un tel y, alors $\forall x \exists y P(x, y)$ est faux.

Pour voir si $\exists x \forall y P(x, y)$ est vrai, nous *parcourons* les valeurs de x jusqu'à ce que nous trouvions un x pour qui $P(x, y)$ est toujours vrai quand on boucle à travers toutes les valeurs pour y. Une fois que nous trouvons un tel x, nous sachez que $\exists x \forall y P(x, y)$ est vrai. Si nous ne frappons jamais un tel x, alors nous savons que $\exists x \forall y P(x, y)$ est faux.

Enfin, pour voir si $\exists x \exists y P(x, y)$ est vrai, nous *parcourons* les valeurs de x, où pour chaque x, nous parcourons les valeurs de y jusqu'à ce que nous atteignions un x pour lequel nous frappons un y pour lequel $P(x, y)$ est vrai. La déclaration $\exists x \exists y P(x, y)$ n'est fausse que si nous ne *frappons* jamais un x pour lequel nous frappons un y tel que $P(x, y)$ est vrai.

L'ordre des quantificateurs

De nombreux énoncés mathématiques impliquent de multiples quantifications des fonctions propositionnelles volving plus d'une variable. Il est important de noter que l'ordre des quantificateurs est important, sauf si tous les quantificateurs sont des quantificateurs universels ou tous sont des quantificateurs existentiels.

Ces remarques sont illustrées par les exemples 3 à 5.

EXEMPLE 3 Soit $P(x, y)$ l'énoncé « $x + y = y + x$ ». Quelles sont les valeurs de vérité des quantifications $\forall x \forall y P(x, y)$ et $\forall y \forall x P(x, y)$ où le domaine pour toutes les variables se compose de tous les nombres réels?

Solution: la quantification

$$\forall x \forall y P(x, y)$$

dénote la proposition

"Pour tous les nombres réels x, pour tous les nombres réels y, $x + y = y + x$."

Parce que $P(x, y)$ est vrai pour tous les nombres réels x et y (c'est la loi commutative pour l'addition, qui est un axiome pour les nombres réels - voir Annexe 1), la proposition $\forall x \forall y P(x, y)$ est vrai. Notez que l'instruction $\forall y \forall x P(x, y)$ dit "Pour tous les nombres réels y, pour tous les nombres réels x, $x + y = y + x$. "Cela a la même signification que la déclaration" pour tous les nombres réels x, pour tous les réels les nombres y, $x + y = y + x$. "Autrement dit, $\forall x \forall y P(x, y)$ et $\forall y \forall x P(x, y)$ ont la même signification, et les deux sont vrais. Cela illustre le principe selon lequel l'ordre des quantificateurs universels imbriqués dans une déclaration sans autres quantificateurs peuvent être modifiés sans changer la signification de la déclaration quantifiée. ▲

EXEMPLE 4 Soit $Q(x, y)$ « $x + y = 0$». Quelles sont les valeurs de vérité des quantifications $\exists y \forall x Q(x, y)$ et $\forall x \exists y Q(x, y)$, où le domaine pour toutes les variables se compose de tous les nombres réels?

Solution: la quantification

$\exists y \forall x Q(x, y)$

dénote la proposition

"Il y a un vrai nombre y tel que pour chaque nombre réel x, $Q(x, y)$."

Quelle que soit la valeur de y choisie, il n'y a qu'une seule valeur de x pour laquelle $x + y = 0$. Parce que il n'y a pas de nombre réel y tel que $x + y = 0$ pour tous les nombres réels x, l'instruction $\exists y \forall x Q(x, y)$ c'est faux.

La quantification

$\forall x \exists y Q(x, y)$

dénote la proposition

"Pour chaque nombre réel x, il existe un nombre réel y tel que $Q(x, y)$."

Étant donné un nombre réel x, il existe un nombre réel y tel que $x + y = 0$; à savoir, $y = -x$. Par conséquent, l'énoncé $\forall x \exists y Q(x, y)$ est vrai. ▲

Soyez prudent avec la commande d'existentiel et quantificateurs universels!

L'exemple 4 illustre que l'ordre dans lequel les quantificateurs apparaissent fait une différence. L'état- Les éléments $\exists y \forall x P(x, y)$ et $\forall x \exists y P(x, y)$ ne sont pas logiquement équivalents. La déclaration $\exists y \forall x P(x, y)$ est vrai si et seulement s'il y a un y qui rend vrai $P(x, y)$ pour chaque x. Donc, pour cette déclaration être vrai, il doit y avoir une valeur particulière de y pour laquelle $P(x, y)$ est vrai quel que soit le choix de x. En revanche, $\forall x \exists y P(x, y)$ est vrai si et seulement si pour chaque valeur de x il y a une valeur de y pour lequel $P(x, y)$ est vrai. Donc, pour que cette affirmation soit vraie, peu importe quel x vous choisissez, il doit y avoir une valeur de y (éventuellement en fonction du x *que* vous choisissez) pour laquelle $P(x, y)$ est vrai. En d'autres termes, dans le second cas, y peut dépendre de x, alors que dans le premier cas, y est une constante indépendant de x.

De ces observations, il s'ensuit que si $\exists y \forall x P(x, y)$ est vrai, alors $\forall x \exists y P(x, y)$ doit être vrai aussi. Cependant, si $\forall x \exists y P(x, y)$ est vrai, il n'est pas nécessaire que $\exists y \forall x P(x, y)$ soit vrai. (Voir les exercices supplémentaires 30 et 31.)

Le tableau 1 résume la signification des différentes quantifications possibles impliquant deux variables.

Les quantifications de plus de deux variables sont également courantes, comme l'illustre l'exemple 5.

EXEMPLE 5 Soit $Q(x, y, z)$ l'énoncé « $x + y = z$ ». Quelles sont les valeurs de vérité des énoncés $\forall x \forall y \exists z Q(x, y, z)$ et $\exists z \forall x \forall y Q(x, y, z)$, où le domaine de toutes les variables se compose de tous nombres réels?

Solution: Supposons que x et y soient des valeurs affectées. Il existe alors un vrai nombre z tel que $x + y = z$. Par conséquent, la quantification

$\forall x \forall y \exists z Q(x, y, z)$,

quelle est la déclaration

"Pour tous les nombres réels x et pour tous les nombres réels y, il existe un nombre réel z tel que $x + y = z$, "

TABLEAU 1 **Quantifications de deux variables.**

Déclaration	*Quand c'est vrai?*	*Quand est-ce faux?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ est vrai pour chaque paire x, y .	Il y a une paire x, y pour qui $P(x, y)$ est fausse.
$\forall x \exists y P(x, y)$	Pour chaque x, il y a un y pour qui $P(x, y)$ est vrai.	Il y a un x tel que $P(x, y)$ est faux pour chaque y .
$\exists x \forall y P(x, y)$	Il y a un x pour lequel $P(x, y)$ est vrai pour chaque y .	Pour chaque x, il y a un y pour qui $P(x, y)$ est fausse.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	Il y a une paire x, y pour laquelle $P(x, y)$ est vrai.	$P(x, y)$ est faux pour chaque paire x, y .

est vrai. L'ordre de quantification ici est important, car la quantification

$$\exists z \forall x \forall y Q(x, y, z),$$

quelle est la déclaration

"Il y a un vrai nombre z tel que pour tous les nombres réels x et pour tous les nombres réels y, il est vrai que $x + y = z$, "

est faux, car aucune valeur de z ne satisfait l'équation $x + y = z$ pour toutes les valeurs de x et y . ▲

Traduction d'instructions mathématiques en instructions Implication de quantificateurs imbriqués

Les énoncés mathématiques exprimés en anglais peuvent être traduits en expressions logiques, comme Les exemples 6 à 8 montrent.

EXEMPLE 6 Traduire l'énoncé «La somme de deux entiers positifs est toujours positive» en une logique expression.

Solution: pour traduire cette déclaration en une expression logique, nous la réécrivons d'abord afin que quantificateurs et un domaine sont affichés: "Pour chaque deux entiers, si ces entiers sont tous les deux positifs, alors la somme de ces entiers est positive. »Ensuite, nous introduisons les variables x et y pour obtenir« Pour tous les entiers positifs x et y , $x + y$ est positif. »Par conséquent, nous pouvons exprimer cette déclaration comme

$$\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow (x + y > 0)),$$

où le domaine pour les deux variables se compose de tous les entiers.Notez que nous pourrions également traduire ceci en utilisant les entiers positifs comme domaine.Ensuite, la déclaration «La somme de deux positifs entiers est toujours positif »devient« Pour chaque deux entiers positifs, la somme de ces entiers est positif. Nous pouvons l'exprimer comme

$$\forall x \forall y (x + y > 0),$$

où le domaine pour les deux variables se compose de tous les entiers positifs. ▲

Exemple 7 Traduire la mention « Chaque nombre réel sauf zéro a une inverse multiplicatif. » (A **mul- l'inverse tiplicatif** d'un nombre réel x est un nombre réel y tel que $xy = 1$.)

Solution: Nous réécrivons d'abord ceci comme «Pour chaque nombre réel x sauf zéro, x a un multiplicatif inverse. "Nous pouvons réécrire ceci comme" Pour chaque nombre réel x , si $x = 0$, alors il existe un réel nombre y tel que $xy = 1$. "Cela peut être réécrit comme

$$\forall x\, ((x = 0\,) \rightarrow \exists y\, (xy = 1\,)).$$

▲

Un exemple que vous connaissez peut-être est le concept de limite, qui est important dans calcul.

EXEMPLE 8 (***Nécessite un calcul***) Utilisez des quantificateurs pour exprimer la définition de la limite d'une valeur réelle fonction $f(x)$ d'une variable réelle x en un point a de son domaine.

Solution: Rappelez-vous que la définition de la déclaration

$$\lim_{x \rightarrow a} f(x) = L$$

est: Pour tout nombre réel $\epsilon > 0$, il existe un nombre réel $\delta > 0$ tel que $| f(x) - L | < \epsilon$ chaque fois que $0 < | x - a | < \delta$. Cette définition d'une limite peut être formulée en termes de quantificateurs par

$$\forall \epsilon\, \exists \delta\, \forall x\, (\, 0 < | x - a | < \delta \rightarrow | f(x) - L | < \epsilon),$$

où le domaine pour les variables δ et ϵ *se* compose de tous les nombres réels positifs et pour x *se* compose de tous les nombres réels.

Cette définition peut également être exprimée comme

$$\forall \epsilon > 0\, \exists \delta > 0\, \forall x\, (\, 0 < | x - a | < \delta \rightarrow | f(x) - L | < \epsilon)$$

lorsque le domaine des variables ϵ et δ *se* compose de tous les nombres réels, plutôt que du seul positif nombres réels. [Ici, des quantificateurs restreints ont été utilisés. Rappelons que $\forall x > 0\ P(x)$ signifie que pour tout x avec $x > 0$, $P(x)$ est vrai.]

▲

Traduction des quantificateurs imbriqués en anglais

Les expressions avec des quantificateurs imbriqués exprimant des déclarations en anglais peuvent être assez compliquées. La première étape de la traduction d'une telle expression consiste à écrire ce que les quantificateurs et les prédicats dans l'expression signifie. L'étape suivante consiste à exprimer ce sens dans une phrase plus simple. Cette est illustré dans les exemples 9 et 10.

EXEMPLE 9 Traduire la déclaration

$$\forall x\, (C(x) \lor \exists y\, (C(y) \land F(x, y)))$$

en anglais, où $C(x)$ est « x a un ordinateur», $F(x, y)$ est « x et y sont amis» et le domaine pour x et y *se* compose de tous les élèves de votre école.

Solution: la déclaration indique que pour chaque élève x de votre école, x a un ordinateur ou est un étudiant y tel que y a un ordinateur et x et y sont amis. En d'autres termes, chaque élève dans votre école a un ordinateur ou a un ami qui a un ordinateur.

▲

EXEMPLE 10 Traduire la déclaration

$$\exists x\, \forall y\, \forall z\, ((F(x, y) \land F(x, z) \land (y = z)) \rightarrow \neg F(y, z))$$

en anglais, où $F(a, b)$ signifie *que a* et b sont amis et que le domaine pour x, y et z *se* compose de tous les élèves de votre école.

Solution: Nous examinons d'abord l'expression $(F(x, y) \land F(x, z) \land (y = z)) \rightarrow \neg F(y, z)$. Cette l'expression dit que si les étudiants x et y sont amis, et les étudiants x et z sont amis, et de plus, si y et z ne sont pas le même élève, alors y et z ne sont pas amis. Il s'ensuit que l'énoncé original, qui est quantifié trois fois, dit qu'il y a un étudiant x tel que pour tous étudiants y et tous les étudiants z autres que y , si x et y sont amis et x et z sont amis, alors y

et z ne sont pas amis. En d'autres termes, il y a un élève dont aucun ami n'est également ami avec l'un l'autre. ▲

Traduire les phrases anglaises en expressions logiques

Dans la section 1.4, nous avons montré comment les quantificateurs peuvent être utilisés pour traduire des phrases en expressions logiques. sions. Cependant, nous avons évité les phrases dont la traduction en expressions logiques nécessitait la utilisation de quantificateurs imbriqués. Nous abordons maintenant la traduction de ces phrases.

EXEMPLE 11 Exprimez la déclaration «Si une personne est une femme et est un parent, alors cette personne est mère »comme une expression logique impliquant des prédicats, des quantificateurs avec un domaine composé de tous les gens et les connecteurs logiques.

Solution: L'énoncé «Si une personne est une femme et qu'elle est un parent, alors cette personne est mère "peut être exprimée par" Pour chaque personne x , si la personne x est une femme et que la personne x est un parent, alors il existe une personne y telle que la personne x est la mère de la personne y . »Nous introduisons la fonctions propositionnelles $F(x)$ pour représenter « x est une femme», $P(x)$ pour représenter « x est un parent», et $M(x, y)$ pour représenter « x est la mère de y ». La déclaration d'origine peut être représentée comme

$$\forall x ((F(x) \wedge P(x)) \rightarrow \exists y M(x, y)).$$

En utilisant la règle de quantification nulle dans la partie (b) de l'exercice 47 de la section 1.4, nous pouvons déplacer $\exists y$ vers la gauche pour qu'elle apparaisse juste après $\forall x$, car y n'apparaît pas dans $F(x) \wedge P(x)$. On obtient l'expression logiquement équivalente

$$\forall x \exists y ((F(x) \wedge P(x)) \rightarrow M(x, y)).$$ ▲

EXEMPLE 12 Exprimer l'énoncé «Tout le monde a exactement un meilleur ami» comme une expression logique impliquant prédicats, quantificateurs avec un domaine composé de toutes les personnes et connecteurs logiques.

Solution: L'énoncé «Tout le monde a exactement un meilleur ami» peut être exprimé comme «Pour chaque la personne x , la personne x a exactement un meilleur ami. "En présentant le quantificateur universel, nous voyons que cette déclaration est la même que «$\forall x$ (la personne x a exactement un meilleur ami)», où le domaine se compose de toutes les personnes.

Dire que x a exactement un meilleur ami signifie qu'il y a une personne y qui est le meilleur ami de x , et de plus que pour chaque personne z , si la personne z n'est pas la personne y , alors z n'est pas le meilleur ami de x . Lorsque nous introduisons le prédicat $B(x, y)$ pour être la déclaration « y est le meilleur ami de x ", la déclaration selon laquelle x a exactement un meilleur ami peut être représentée comme

$$\exists y (B(x, y) \wedge \forall z ((z = y) \rightarrow \neg B(x, z))).$$

Par conséquent, notre déclaration originale peut être exprimée comme suit:

$$\forall x \exists y (B(x, y) \wedge \forall z ((z = y) \rightarrow \neg B(x, z))).$$

[Notez que nous pouvons écrire cette déclaration sous la forme $\forall x \exists! y B(x, y)$, où $\exists!$ est le «quantificateur d'unicité» définis à la section 1.4.] ▲

EXEMPLE 13 Utilisez des quantificateurs pour exprimer la déclaration «Il y a une femme qui a pris un vol compagnie aérienne dans le monde.

Solution: Soit $P(w, f)$ « w a pris f » et $Q(f, a)$ « f est un vol sur a ». On peut exprimer la déclaration comme

$$\exists w \forall a \exists f (P(w, f) \wedge Q(f, a)),$$

où les domaines du discours pour w, f et a *se* composent de toutes les femmes du monde, de tous les avions et toutes les compagnies aériennes, respectivement.

La déclaration pourrait également être exprimée comme suit:

$$\exists w \forall a \exists f R(w, f, a),$$

où $R(w, f, a)$ est « w a pris f sur a ». Bien que ce soit plus compact, il obscurcit quelque peu les relations entre les variables. Par conséquent, la première solution est généralement préférable. ▲

Négation des quantificateurs imbriqués

Les déclarations impliquant des quantificateurs imbriqués peuvent être annulées en appliquant successivement les règles les déclarations négatives impliquant un seul quantificateur.Ceci est illustré dans les exemples 14 à 16.

EXEMPLE 14 Exprimer la négation de l'instruction $\forall x \exists y (xy = 1)$ *de* sorte qu'aucune négation ne précède un quantificateur.

Solution: en appliquant successivement les lois de De Morgan pour les quantificateurs du tableau 2 de Section 1.4, nous pouvons déplacer la négation en $\neg\forall x \exists y (xy = 1)$ *à l'* intérieur de tous les quantificateurs. Nous trouvons que $\neg\forall x \exists y (xy = 1)$ est équivalent à $\exists x \neg\exists y (xy = 1)$, ce qui équivaut à $\exists x \forall y \neg (xy = 1)$. Parce que $\neg (xy = 1)$ peut être exprimé plus simplement par xy = 1, nous concluons que notre négation peut être exprimée par $\exists x \forall y (xy = 1)$. ▲

EXEMPLE 15 Utilisez des quantificateurs pour exprimer la déclaration selon laquelle «il n'existe pas de femme qui a vol sur toutes les compagnies aériennes du monde.

Solution: cette déclaration est la négation de la déclaration «Il y a une femme qui a pris un vol sur chaque compagnie aérienne dans le monde "de l'exemple 13. Par l'exemple 13, notre déclaration peut être exprimée par $\neg\exists w \forall a \exists f (P(w, f) \wedge Q(f, a))$, où $P(w, f)$ est « w a pris f » et $Q(f, a)$ est « f est un vol sur a ». En appliquant successivement les lois de De Morgan pour les quantificateurs du tableau 2 de la section 1.4 pour déplacer la négation à l'intérieur des quantificateurs successifs et en appliquant la méthode de De Morgan loi pour nier une conjonction à la dernière étape, nous constatons que notre déclaration est équivalente à chaque de cette séquence de déclarations:

$$\begin{aligned}\forall w \neg\forall a \exists f (P(w, f) \wedge Q(f, a)) &\equiv \forall w \exists a \neg\exists f (P(w, f) \wedge Q(f, a))\\ &\equiv \forall w \exists a \forall f \neg (P(w, f) \wedge Q(f, a))\\ &\equiv \forall w \exists a \forall f (\neg P(w, f) \vee \neg Q(f, a)).\end{aligned}$$

Cette dernière déclaration déclare: «Pour chaque femme, il existe une compagnie aérienne telle que pour tous les vols, cette la femme n'a pas pris ce vol ou ce vol ne fait pas partie de cette compagnie aérienne. » ▲

EXEMPLE 16 (*Nécessite un calcul*) Utilisez des quantificateurs et des prédicats pour exprimer le fait que $\lim_{x\to a} f(x)$ ne n'existe pas où $f(x)$ est une fonction à valeur réelle d'une variable réelle x et a appartient au domaine de f .

Solution: Dire que $\lim_{x\to a} f(x)$ n'existe pas signifie que pour tous les nombres réels L , $\lim_{x\to a} f(x) = L$. En utilisant l'exemple 8, l'instruction $\lim_{x\to a} f(x) = L$ peut être exprimée comme

$$\neg\forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon).$$

En appliquant successivement les règles de négation des expressions quantifiées, nous construisons cette séquence de déclarations équivalentes

$$\begin{aligned}&\neg\forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)\\ &\quad\equiv \exists \epsilon > 0 \neg\exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)\\ &\quad\equiv \exists \epsilon > 0 \forall \delta > 0 \neg\forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)\\ &\quad\equiv \exists \epsilon > 0 \forall \delta > 0 \exists x \neg (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon)\\ &\quad\equiv \exists \epsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon).\end{aligned}$$

Dans la dernière étape, nous avons utilisé l'équivalence $\neg(p \rightarrow q) \equiv p \wedge \neg q$, qui découle de la cinquième équivalence dans le tableau 7 de la section 1.3.

Parce que l'énoncé « $\lim_{x\to a} f(x)$ n'existe pas» signifie pour tous les nombres réels L , $\lim_{x\to a} f(x) = L$, cela peut être exprimé comme

$$\forall L \exists \epsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \wedge |f(x) - L| \geq \epsilon).$$

Cette dernière affirmation dit que pour chaque nombre réel L, il existe un nombre réel $\epsilon > 0$ tel que pour tout nombre réel $\delta > 0$, il existe un nombre réel x tel que $0 < |x - a| < \delta$ et $|f(x) - L| \geq \epsilon$. ▲

Des exercices

1. Traduire ces déclarations en anglais, où le domaine pour chaque variable se compose de tous les nombres réels.

à votre école. Exprimez chacune de ces quantifications en Anglais.

a) $\forall x \exists y (x < y)$
b) $\forall x \forall y (((x \geq 0) \wedge (y \geq 0)) \rightarrow (xy \geq 0))$
c) $\forall x \forall y \exists z (xy = z)$

2. Traduisez ces déclarations en anglais, où le domaine pour chaque variable se compose de tous les nombres réels.

a) $\exists x \forall y (xy = y)$
b) $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$
c) $\forall x \forall y \exists z (x = y + z)$

3. Soit $Q(x, y)$ la déclaration « x a envoyé un e-mail sage to y ", où le domaine pour x et y *se* compose de tous les élèves de votre classe. Exprimez chacune de ces quantifications en anglais.

a) $\exists x \exists y Q(x, y)$ **b)** $\exists x \forall y Q(x, y)$
c) $\forall x \exists y Q(x, y)$ **d)** $\exists y \forall x Q(x, y)$
e) $\forall y \exists x Q(x, y)$ **f)** $\forall x \forall y Q(x, y)$

4. Soit $P(x, y)$ l'énoncé «L'élève x a pris le cours y ", où le domaine de x comprend tous les étudiants de votre classe et pour y *se* compose de tous les cours d'informatique

a) $\exists x \exists y P(x, y)$ **b)** $\exists x \forall y P(x, y)$
c) $\forall x \exists y P(x, y)$ **d)** $\exists y \forall x P(x, y)$
e) $\forall y \exists x P(x, y)$ **f)** $\forall x \forall y P(x, y)$

5. Soit $W(x, y)$ signifie que l'élève x a visité le site Web y, où le domaine pour x *se* compose de tous les étudiants de votre l'école et le domaine pour y *se* compose de tous les sites Web. Ex-appuyez sur chacune de ces déclarations par un simple tence.

a) W (Sarah Smith, www.att.com)
b) $\exists x W(x$, www.imdb.org)
c) $\exists y W$ (José Orez, y)
d) $\exists y$ (W (Ashok Puri, y) $\wedge$ W (Cindy Yoon, y))
e) $\exists y \forall z$ (y = (David Belcher) $\wedge$ (W (David Belcher, z) $\rightarrow W(y, z)$))
f) $\exists x \exists y \forall z ((x = y) \wedge (W(x, z) \leftrightarrow W(y, z)))$

6. Soit $C(x, y)$ signifie que l'élève x est inscrit dans la classe y, où le domaine pour x *se* compose de tous les étudiants de votre l'école et le domaine pour y *se* compose de toutes les classes étant

donné à votre école. Exprimez chacune de ces déclarations par une simple phrase en anglais.

a) C (Randy Goldberg, CS 252)
b) $\exists x C(x$, Math 695)
c) $\exists y C$ (Carol Sitea, y)
d) $\exists x$ (C (x , Math 222) $\wedge$ C (x , CS 252))
e) $\exists x \exists y \forall z ((x = y) \wedge (C(x, z) \rightarrow C(y, z)))$
f) $\exists x \exists y \forall z ((x = y) \wedge (C(x, z) \leftrightarrow C(y, z)))$

7. Soit $T(x, y)$ signifie que l'élève x aime la cuisine y, où le domaine pour x *se* compose de tous les élèves de votre école et le domaine pour y comprend toutes les cuisines. Exprimez chacun ces déclarations par une simple phrase en anglais.

a) $\neg T$ (Abdallah Hussein, japonais)
b) $\exists x T(x$, coréen) $\wedge \forall x T(x$, mexicain)
c) $\exists y (T$ (Monique Arsenault, $y) \vee$ T (Jay Johnson, y))
d) $\forall x \forall z \exists y ((x = z) \rightarrow \neg (T(x, y) \wedge T(z, y)))$
e) $\exists x \exists z \forall y (T(x, y) \leftrightarrow T(z, y))$
f) $\forall x \forall z \exists y (T(x, y) \leftrightarrow T(z, y))$

8. Soit $Q(x, y)$ l'énoncé «l'élève x a été un testant sur quiz montrer y . "Exprimez chacune de ces phrases en termes de $Q(x, y)$, de quantificateurs et de connecteurs logiques, où le domaine pour x *se* compose de tous les étudiants de votre l'école et pour y *se* compose de toutes les émissions de quiz à la télévision.

a) Il y a un élève dans votre école qui a été testant sur un quiz télévisé.
b) Aucun élève de votre école n'a jamais été candidat sur un quiz télévisé.
c) Il y a un élève dans votre école qui a été testant sur *Jeopardy* et sur *Wheel of Fortune* .
d) Chaque émission télévisée de quiz a eu un étudiant de votre école en tant que candidat.
e) Au moins deux élèves de votre école ont été testants sur *Jeopardy* .

9. Soit $L(x, y)$ l'énoncé « x aime y », où le do-principal pour x et y est composé de toutes les personnes dans le monde. Utilisez des quantificateurs pour exprimer chacune de ces déclarations.

a) Tout le monde aime Jerry.
b) Tout le monde aime quelqu'un.
c) Il y a quelqu'un que tout le monde aime.
d) Personne n'aime tout le monde.
e) Il y a quelqu'un que Lydia n'aime pas.
f) Il y a quelqu'un que personne n'aime.
g) Il y a exactement une personne que tout le monde aime.
h) Il y a exactement deux personnes que Lynn aime.
i) Tout le monde s'aime.
j) Il y a quelqu'un qui n'aime personne à part lui-même ou elle-même.

10. Soit $F(x, y)$ l'énoncé « x peut tromper y », où le Le domaine se compose de toutes les personnes dans le monde. Utiliser des quantificateurs pour exprimer chacune de ces déclarations.

a) Tout le monde peut tromper Fred.
b) Evelyn peut tromper tout le monde.
c) Tout le monde peut tromper quelqu'un.
h) Il y a exactement une personne que tout le monde peut tromper.
i) Personne ne peut se tromper.
j) Il y a quelqu'un qui peut tromper exactement une personne en plus de lui-même.

11. Soit $S(x)$ le prédicat « x est un étudiant», $F(x)$ le prédicat icate « x est membre du corps professoral» et $A(x, y)$ le prédicat " X a posé une question à y ", où le domaine se compose de toutes les personnes associées à votre école. Utilisez des quantificateurs pour exprimer chacune de ces déclarations.

a) Lois a posé une question au professeur Michaels.
b) Chaque étudiant a posé une question au professeur Gross.
c) Chaque membre du corps professoral a demandé au professeur Miller une question ou une question de Pro-le fesseur Miller.
d) Un étudiant n'a demandé à aucun membre du corps professoral question.
e) Il y a un membre du corps professoral qui n'a jamais été invité une question d'un étudiant.
f) Un étudiant a demandé à chaque membre du corps professoral tion.
g) Un membre du corps professoral a demandé à tous les autres membre du corps professoral une question.
h) Un élève n’a jamais posé de question à un membre de la faculté.

12. Soit $I(x)$ la déclaration « x a une connexion Internet» et $C(x, y)$ soit la déclaration « x et y ont discuté Internet ", où le domaine des variables x et y se compose de tous les élèves de votre classe. Utilisez des quantificateurs pour exprimer chacune de ces déclarations.

a) Jerry n'a pas de connexion Internet.
b) Rachel n'a pas discuté sur Internet avec Chelsea.
c) Jan et Sharon n'ont jamais discuté sur Internet.
d) Personne dans la classe n'a discuté avec Bob.
e) Sanjay a discuté avec tout le monde sauf Joseph.
f) Quelqu'un dans votre classe n'a pas de connexion Internet nection.
g) Tout le monde dans votre classe n’a pas de connexion Internet tion.
h) Exactement un élève de votre classe a une connexion Internet nection.
i) Tout le monde, sauf un élève de votre classe, a un connexion ternet.
j) Tout le monde dans votre classe avec une connexion Internet a discuté sur Internet avec au moins un autre étudiant dans votre classe.
k) Quelqu'un dans votre classe a une connexion Internet mais n'a discuté avec personne d'autre dans votre classe.
l) Il y a deux élèves dans votre classe qui n'ont pas bavardé entre eux sur Internet.
m) Un élève de votre classe a discuté avec tout le monde dans votre classe sur Internet.
n) Il y a au moins deux élèves dans votre classe qui ont

d) Personne ne peut tromper tout le monde.
e) Tout le monde peut être trompé par quelqu'un.
f) Personne ne peut tromper Fred et Jerry.
g) Nancy peut tromper exactement deux personnes.

pas discuté avec la même personne de votre classe.
o) Il y a deux élèves dans la classe qui entre eux
ont discuté avec tout le monde dans la classe.

13. Soit *M (x, y)* « *x* a envoyé à *y* un message électronique» et *T (x, y)* soit « *x* a téléphoné *y* », où le domaine con-
les listes de tous les élèves de votre classe. Utilisez des quantificateurs pour appuyez sur chacune de ces déclarations. (Supposons que tous les e-mails les messages envoyés sont reçus, ce qui n'est pas le comme les choses fonctionnent souvent.)

a) Chou n'a jamais envoyé de message électronique à Koko.
b) Arlene n'a jamais envoyé de message électronique ou de a téléphoné à Sarah.
c) José n'a jamais reçu de message électronique de Deb- orah.
d) Chaque élève de votre classe a envoyé un e-mail sage à Ken.
e) Personne dans ta classe n'a téléphoné à Nina.
f) Tout le monde dans votre classe a téléphoné à Avi ou lui a envoyé un e-mail.
g) Il y a un élève dans ta classe qui a envoyé tout le monde sinon dans votre classe un e-mail.
h) Il y a quelqu'un dans votre classe qui a envoyé un e-mail ou téléphoné à tout le monde dans votre classe.
i) Il y a deux élèves différents dans votre classe qui se sont envoyés des courriels.
j) Il y a un étudiant qui s'est envoyé lui-même un message électronique.
k) Il y a un élève dans votre classe qui n'a pas reçu un message électronique de quelqu'un d'autre dans la classe et qui n'a été appelé par aucun autre élève du classe.
l) Chaque élève de la classe a reçu un e- message électronique ou reçu un appel téléphonique autre élève de la classe.
m) Il y a au moins deux élèves dans votre classe de telle sorte que un étudiant a envoyé l'autre e-mail et le second étudiant a téléphoné au premier étudiant.
n) Il y a deux élèves différents dans votre classe qui entre eux ont envoyé un message électronique ou a téléphoné à tout le monde dans la classe.

14. Utilisez des quantificateurs et des prédicats avec plus d'un capable d'exprimer ces déclarations.

a) Il y a un étudiant dans cette classe qui peut parler l'hindi.
b) Chaque élève de cette classe fait du sport.
c) Un élève de cette classe a visité l'Alaska mais a pas visité Hawaï.
d) Tous les élèves de cette classe ont appris au moins un programme langue de programmation.
e) Il y a un étudiant dans cette classe qui a suivi tous les cours offerts par l'un des départements de ce école.
f) Un élève de cette classe a grandi dans la même ville comme exactement un autre élève de cette classe.
g) Chaque élève de cette classe a discuté avec au moins un autre étudiant dans au moins un groupe de discussion.

15. Utilisez des quantificateurs et des prédicats avec plus d'un capable d'exprimer ces déclarations.

a) Chaque étudiant en informatique a besoin d'un cours de mathématiques crètes.
b) Il y a un étudiant dans cette classe qui possède un ordinateur.
c) Chaque élève de cette classe a suivi au moins un cours cours de science informatique.
d) Il y a un étudiant dans cette classe qui a suivi au moins un cours d'informatique.
e) Chaque élève de cette classe a été dans chaque bâtiment sur le campus.
f) Il y a un étudiant dans cette classe qui a été dans tous les chambre d'au moins un bâtiment sur le campus.
g) Chaque élève de cette classe a fréquenté au moins un salle de chaque bâtiment sur le campus.

16. Un cours de mathématiques discret contient 1 cours de mathématiques jor qui est un étudiant de première année, 12 majors en mathématiques qui sont étudiants de deuxième année, 15 majeures en informatique qui sont mores, 2 majors mathématiques qui sont juniors, 2 ordinateur majors scientifiques juniors et 1 informatique major qui est un senior. Exprimez chacune de ces déclarations dans termes de quantificateurs, puis déterminer sa valeur de vérité.

a) Il y a un étudiant dans la classe qui est un junior.
b) Chaque élève de la classe est majeur en informatique.
c) Il y a un élève dans la classe qui n'est ni mathématicien ématique majeur ni junior.
d) Chaque élève de la classe est soit un étudiant en deuxième année ou un majeure en informatique.
e) Il y a un majeur tel qu'il y a un élève dans la classe dans chaque année d'études avec cette majeure.

17. Exprimez chacune de ces spécifications de système en utilisant cates, quantificateurs et connecteurs logiques, si nécessaire.

a) Chaque utilisateur a accès à exactement une boîte aux lettres.
b) Il existe un processus qui continue de s'exécuter pendant toutes les erreurs conditions que si le noyau fonctionne correctement.
c) Tous les utilisateurs du réseau du campus peuvent accéder à tous les sites dont l'URL a une extension .edu.
∗ **d)** Il existe exactement deux systèmes qui surveillent chaque serveur mote.

18. Exprimez chacune de ces spécifications de système en utilisant cates, quantificateurs et connecteurs logiques, si nécessaire.

a) Au moins une console doit être accessible à chaque condition de défaut.
b) L'adresse e-mail de chaque utilisateur peut être récupérée chaque fois que l'archive contient au moins un message envoyé par chaque utilisateur du système.
c) Pour chaque brèche de sécurité, il existe au moins un mécanisme nisme qui peut détecter cette violation si et seulement s'il y a un processus qui n'a pas été compromis.
d) Il y a au moins deux chemins reliant tous les deux dis- points de terminaison tincts sur le réseau.
e) Personne ne connaît le mot de passe de chaque utilisateur du système. sauf pour l'administrateur système, qui sait tous les mots de passe. [

19. Exprimez chacune de ces affirmations en utilisant des opérateurs, prédicats et quantificateurs logiques, où le domaine se compose de tous les entiers.

a) La somme de deux entiers négatifs est négative.
b) La différence de deux entiers positifs n'est pas nécessaire positif.

c) La somme des carrés de deux entiers est supérieure à ou égal au carré de leur somme.

d) La valeur absolue du produit de deux entiers est le produit de leurs valeurs absolues.

20. Exprimez chacune de ces déclarations en utilisant des prédicats, tificateurs, connecteurs logiques et opérateurs mathématiques où le domaine se compose de tous les entiers.

a) Le produit de deux entiers négatifs est positif.

b) La moyenne de deux entiers positifs est positive.

c) La différence de deux entiers négatifs n'est pas nécessaire sairement négatif.

d) La valeur absolue de la somme de deux entiers ne pas dépasser la somme des valeurs absolues de ces entiers.

21. Utilisez des prédicats, des quantificateurs, des connecteurs logiques et opérateurs mathématiques pour exprimer la déclaration selon laquelle Chaque entier positif est la somme des carrés de quatre tegers.

22. Utilisez des prédicats, des quantificateurs, des connecteurs logiques et opérateurs mathématiques pour exprimer la déclaration selon laquelle il est un entier positif qui n'est pas la somme de trois carrés.

23. Exprimez chacun de ces énoncés mathématiques en utilisant prédicats, quantificateurs, connecteurs logiques et matrices opérateurs matiques.

a) Le produit de deux nombres réels négatifs est positif.

b) La différence entre un nombre réel et lui-même est nulle.

c) Chaque nombre réel positif a exactement deux carrés les racines.

d) Un nombre réel négatif n'a pas de racine carrée c'est un vrai nombre.

24. Traduisez chacune de ces quantifications imbriquées en un déclaration glish qui exprime un fait mathématique. le domaine dans chaque cas se compose de tous les nombres réels.

a) $\exists x \forall y (x + y = y)$

b) $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$

c) $\exists x \exists y (((x \leq 0) \wedge (y \leq 0)) \wedge (x - y > 0))$

d) $\forall x \forall y ((x = 0) \wedge (y = 0) \leftrightarrow (xy = 0))$

25. Traduisez chacune de ces quantifications imbriquées en un déclaration glish qui exprime un fait mathématique. le domaine dans chaque cas se compose de tous les nombres réels.

a) $\exists x \forall y (xy = y)$

b) $\forall x \forall y (((x < 0) \wedge (y < 0)) \rightarrow (xy > 0))$

c) $\exists x \exists y ((x^2 > y) \wedge (x < y))$

d) $\forall x \forall y \exists z (x + y = z)$

26. Soit $Q(x, y)$ l'énoncé « $x + y = x - y$ ». Si le do- principal pour les deux variables se compose de tous les entiers, quels sont les valeurs de vérité?

a) $Q(1, 1)$ **b)** $Q(2, 0)$

c) $\forall y Q(1, y)$ **d)** $\exists x Q(x, 2)$

e) $\exists x \exists y Q(x, y)$ **f)** $\forall x \exists y Q(x, y)$

g) $\exists y \forall x Q(x, y)$ **h)** $\forall y \exists x Q(x, y)$

i) $\forall x \forall y Q(x, y)$

27. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine pour toutes les variables se compose de tous les entiers.

a) $\forall n \exists m (n^2 < m)$ **b)** $\exists n \forall m (n < m^2)$

c) $\forall n \exists m (n + m = 0)$ **d)** $\exists n \forall m (nm = m)$

e) $\exists n \exists m (n^2 + m^2 = 5)$ **f)** $\exists n \exists m (n^2 + m^2 = 6)$

g) $\exists n \exists m (n + m = 4 \wedge n - m = 1)$

h) $\exists n \exists m (n + m = 4 \wedge n - m = 2)$

i) $\forall n \forall m \exists p (p = (m + n) / 2)$

28. Déterminez la valeur de vérité de chacune de ces déclarations si le domaine de chaque variable est constitué de tous les nombres réels.

a) $\forall x \exists y (x^2 = y)$ **b)** $\forall x \exists y (x = y^2)$

c) $\exists x \forall y (xy = 0)$ **d)** $\exists x \exists y (x + y = y + x)$

e) $\forall x (x = 0 \rightarrow \exists y (xy = 1))$

f) $\exists x \forall y (y = 0 \rightarrow xy = 1)$

g) $\forall x \exists y (x + y = 1)$

h) $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$

i) $\forall x \exists y (x + y = 2 \wedge 2x - y = 1)$

j) $\forall x \forall y \exists z (z = (x + y) / 2)$

29. Supposons le domaine de la fonction propositionnelle $P(x, y)$ se compose des paires x et y, où x est 1, 2 ou 3 et y est 1, 2 ou 3. Écrivez ces propositions en utilisant des disjonctions et les conjonctions.

a) $\forall x \forall y P(x, y)$ **b)** $\exists x \exists y P(x, y)$

c) $\exists x \forall y P(x, y)$ **d)** $\forall y \exists x P(x, y)$

30. Réécrivez chacune de ces déclarations afin que les négations poire uniquement dans les prédicats (c'est-à-dire, afin qu'aucune négation est en dehors d'un quantificateur ou d'une expression impliquant logique connecteurs).

a) $\neg \exists y \exists x P(x, y)$ **b)** $\neg \forall x \exists y P(x, y)$

c) $\neg \exists y (Q(y) \wedge \forall x \neg R(x, y))$

d) $\neg \exists y (\exists x R(x, y) \vee \forall x S(x, y))$

e) $\neg \exists y (\forall x \exists z T(x, y, z) \vee \exists x \forall z U(x, y, z))$

31. Exprimez la négation de chacune de ces déclarations afin que tous les symboles de négation précèdent immédiatement les prédicats.

a) $\forall x \exists y \forall z T(x, y, z)$

b) $\forall x \exists y P(x, y) \vee \forall x \exists y Q(x, y)$

c) $\forall x \exists y (P(x, y) \wedge \exists z R(x, y, z))$

d) $\forall x \exists y (P(x, y) \rightarrow Q(x, y))$

32. Exprimez la négation de chacune de ces déclarations afin que tous les symboles de négation précèdent immédiatement les prédicats.

a) $\exists z \forall y \forall x T(x, y, z)$

b) $\exists x \exists y P(x, y) \wedge \forall x \forall y Q(x, y)$

c) $\exists x \exists y (Q(x, y) \leftrightarrow Q(y, x))$

d) $\forall y \exists x \exists z (T(x, y, z) \vee Q(x, y))$

33. Réécrivez chacune de ces déclarations afin que les négations poire uniquement dans les prédicats (c'est-à-dire, afin qu'aucune négation est en dehors d'un quantificateur ou d'une expression impliquant logique connecteurs).

a) $\neg \forall x \forall y P(x, y)$ **b)** $\neg \forall y \exists x P(x, y)$

c) $\neg \forall y \forall x (P(x, y) \vee Q(x, y))$

d) $\neg (\exists x \exists y \neg P(x, y) \wedge \forall x \forall y Q(x, y))$

e) $\neg \forall x (\exists y \forall z P(x, y, z) \wedge \exists z \forall y P(x, y, z))$

34. Trouver un domaine commun pour les variables x, y et z pour laquelle l'énoncé $\forall x \forall y ((x = y) \rightarrow \forall z ((z = x) \vee (z = y)))$ est vrai et un autre domaine pour lequel il est faux.

35. Trouver un domaine commun pour les variables x, y, z, et w pour lequel l'énoncé $\forall x \forall y \forall z \exists w ((w = x) \wedge (w = y) \wedge (w = z))$ est vrai et un autre domaine commun pour ces variables pour lesquelles il est faux.

36. Exprimez chacune de ces déclarations à l'aide de quantificateurs. alors former la négation de la déclaration afin qu'aucune négation ne soit à gauche d'un quantificateur. Ensuite, exprimez la négation dans anglais simple. (N'utilisez pas simplement l'expression «Ce n'est pas le cas. ")

a) Personne n'a perdu plus de mille dollars à la loterie.
b) Il y a un élève dans cette classe qui a discuté avec exactement un autre étudiant.
c) Aucun élève de cette classe n'a envoyé d'e-mail à exactement deux d'autres élèves de cette classe.
d) Un élève a résolu tous les exercices de ce livre.
e) Aucun élève n'a résolu au moins un exercice dans chaque section de ce livre.

37. Exprimez chacune de ces déclarations à l'aide de quantificateurs. alors former la négation de la déclaration afin qu'aucune négation ne soit à gauche d'un quantificateur. Ensuite, exprimez la négation dans anglais simple. (N'utilisez pas simplement l'expression «Ce n'est pas le cas. ")

a) Chaque élève de cette classe a suivi exactement deux cours de cours d'ématisme dans cette école.
b) Quelqu'un a visité tous les pays du monde sauf Libye.
c) Personne n'a gravi toutes les montagnes de l'Himalaya.
d) Chaque acteur de cinéma a été dans un film avec Kevin Bacon ou a été dans un film avec quelqu'un qui a été dans un film avec Kevin Bacon.

38. Exprimez les négations de ces propositions en utilisant des et en anglais.

a) Chaque élève de cette classe aime les mathématiques.
b) Il y a un élève dans cette classe qui n'a jamais vu un ordinateur.
c) Il y a un étudiant dans cette classe qui a suivi tous les cours de mathématiques offert dans cette école.
d) Il y a un étudiant dans cette classe qui a été au moins dans une pièce de chaque bâtiment sur le campus.

39. Trouver un contre-exemple, si possible, à ces universellement déclarations quantifiées, où le domaine pour toutes les variables se compose de tous les entiers.

a) $\forall x \forall y (x^2 = y^2 \rightarrow x = y)$
b) $\forall x \exists y (y^2 = x)$
c) $\forall x \forall y (xy \geq x)$

40. Trouver un contre-exemple, si possible, à ces universellement déclarations quantifiées, où le domaine pour toutes les variables se compose de tous les entiers.

a) $\forall x \exists y (x = 1 / y)$
b) $\forall x \exists y (y^2 - x < 100)$
c) $\forall x \forall y (x^2 = y^3)$

41. Utilisez des quantificateurs pour exprimer la loi associative pour plication de nombres réels.

42. Utilisez des quantificateurs pour exprimer les lois distributives des plication sur l'addition pour les nombres réels.

43. Utilisez des quantificateurs et des connecteurs logiques pour exprimer le fait que chaque polynôme linéaire (c'est-à-dire polynôme de dégree 1) avec des coefficients réels et où le coefficient de x est différent de zéro, a exactement une racine réelle.

44. Utilisez des quantificateurs et des connecteurs logiques pour exprimer le fait qu'un polynôme quadratique avec des coefficients de nombre réel a au plus deux vraies racines.

45. Déterminer la valeur de vérité de l'énoncé $\forall x \exists y (xy = 1)$ si le domaine des variables consiste en

a) les nombres réels non nuls.
b) les entiers non nuls.
c) les nombres réels positifs.

46. Déterminer la valeur de vérité de l'énoncé $\exists x \forall y (x \leq y^2)$ si le domaine des variables consiste en

a) les nombres réels positifs.
b) les entiers.
c) les nombres réels non nuls.

47. Montrer que les deux énoncés $\neg\exists x \forall y P(x, y)$ et $\forall x \exists y \neg P(x, y)$, où les deux quantificateurs sur la première vari- dans $P(x, y)$ ont le même domaine, et les deux quanti- fiers sur la deuxième variable dans $P(x, y)$ ont le même domaine, sont logiquement équivalents.

∗ **48.** Montrer que $\forall x P(x) \vee \forall x Q(x)$ et $\forall x \forall y (P(x) \vee Q(y))$, où tous les quantificateurs ont le même domaine non vide, sont logiquement équivalents. (La nouvelle variable y est utilisée pour combiner correctement les quantifications.)

∗ **49. a)** Montrer que $\forall x P(x) \wedge \exists x Q(x)$ est logiquement équivalent à $\forall x \exists y (P(x) \wedge Q(y))$, où tous les quantificateurs ont le même domaine non vide.

b) Montrer que $\forall x P(x) \vee \exists x Q(x)$ est équivalent à $\forall x \exists y (P(x) \vee Q(y))$, où tous les quantificateurs ont le même domaine non vide.

Une déclaration est sous **forme normale prénex (PNF)** si et seulement si elle est de la forme

$$Q_1 x_1 Q_2 x_2 \cdots Q_k x_k P(x_1, x_2, \ldots, x_k),$$

où chaque Q_i, $i = 1, 2, \ldots, k$, est soit la quantité existentielle ou le quantificateur universel, et $P(x_1, \ldots, x_k)$ est une prédiction icate n'impliquant aucun quantificateur. Par exemple, $\exists x \forall y (P(x, y) \wedge Q(y))$ est sous forme normale *prénex*, alors que $\exists x P(x) \vee \forall x Q(x)$ n'est pas (car les quantificateurs ne se produisent pas tous en premier).

Chaque énoncé formé de variables propositionnelles, prédicats, **T** et **F à l'** aide de connecteurs logiques et de tifiers est équivalent à une déclaration sous forme normale prénex. L'exercice 51 demande une preuve de ce fait.

∗ **50.** Mettez ces déclarations sous forme normale prénex. [*Astuce:* utiliser l'équivalence logique des tableaux 6 et 7 de la section 1.3, Tableau 2 dans la section 1.4, exemple 19 dans la section 1.4, Exercices 45 et 46 de la section 1.4, et exercices 48 et 49.]

a) $\exists x P(x) \vee \exists x Q(x) \vee A$, où A est une proposition non impliquant des quantificateurs.
b) $\neg(\forall x P(x) \vee \forall x Q(x))$
c) $\exists x P(x) \rightarrow \exists x Q(x)$

∗∗ **51.** Montrez comment transformer une déclaration arbitraire en un état- ment sous une forme normale prénex équivalente à la valeur déclaration. (Remarque: une solution formelle de cet exercice nécessite l'utilisation de l'induction structurelle, abordée dans la section 5.3.)

∗ **52.** Exprimez la quantification $\exists! x P(x)$, introduit dans la sec- 1.4, en utilisant des quantifications universelles, des quantités existentielles et opérateurs logiques.

Règles d'inférence

introduction

Plus loin dans ce chapitre, nous étudierons les preuves. Les preuves en mathématiques sont des arguments valables lish la vérité des énoncés mathématiques. Par un **argument** , nous entendons une séquence d'instructions cette fin avec une conclusion. Par **valide** , nous entendons que la conclusion, ou la déclaration finale du , doit découler de la vérité des déclarations ou**prémisses** précédentes de l'argument.
Autrement dit, un argument n'est valable que si et seulement s'il est impossible que toutes les prémisses soient vraies et la conclusion est fausse. Pour déduire de nouvelles déclarations des déclarations que nous avons déjà, nous utilisons règles d'inférence qui sont des modèles pour construire des arguments valides. Les règles d'inférence sont nos outils de base pour établir la vérité des déclarations.

Avant d'étudier les preuves mathématiques, nous examinerons les arguments qui impliquent uniquement des composés propositions. Nous définirons ce que cela signifie pour un argument impliquant des propositions composées être valide. Ensuite, nous introduirons un ensemble de règles d'inférence dans la logique propositionnelle. Celles-ci les règles d'inférence sont parmi les ingrédients les plus importants pour produire des arguments valides. Après nous illustrons comment les règles d'inférence sont utilisées pour produire des arguments valides, nous décrirons certains formes courantes de raisonnement incorrect, appelées **erreurs** , qui conduisent à des arguments invalides.

Après avoir étudié les règles d'inférence en logique propositionnelle, nous introduirons des règles d'inférence pour les déclarations quantifiées. Nous décrirons comment ces règles d'inférence peuvent être utilisées pour produire arguments valides. Ces règles d'inférence pour les déclarations impliquant existentielle et universelle quantificateurs jouent un rôle important dans les preuves en informatique et en mathématiques, bien qu'ils sont souvent utilisés sans être explicitement mentionnés.

Enfin, nous montrerons comment les règles d'inférence pour les propositions et pour les énoncés quantifiés peut être combiné. Ces combinaisons de règles d'inférence sont souvent utilisées ensemble dans des arguments.

Arguments valides dans la logique propositionnelle

Considérons l'argument suivant impliquant des propositions (qui, par définition, est une séquence de propositions):

"Si vous avez un mot de passe actuel, vous pouvez vous connecter au réseau."

"Vous avez un mot de passe actuel."

Donc,

"Vous pouvez vous connecter au réseau."

Nous aimerions déterminer s'il s'agit d'un argument valable. Autrement dit, nous aimerions déterminer si la conclusion «Vous pouvez vous connecter au réseau» doit être vraie lorsque le locaux "Si vous avez un mot de passe actuel, vous pouvez vous connecter au réseau" et "Vous avez un mot de passe actuel "sont tous les deux vrais.

Avant de discuter de la validité de cet argument particulier, nous examinerons sa forme. Utilisez p pour représenter «Vous avez un mot de passe actuel» et q pour représenter «Vous pouvez vous connecter au réseau». Ensuite, l'argument a la forme

$p \to q$
p

$\therefore q$

où $\therefore$ est le symbole qui signifie «donc».

Nous savons que lorsque p et q sont des variables propositionnelles, l'énoncé $((p \to q) \wedge p) \to q$ est une tautologie (voir exercice 10 (c) à la section 1.3).En particulier, lorsque $p \to q$ et p sont tous deux vrai, nous savons que q doit aussi être vrai. Nous disons que cette forme d'argument est **valable** parce que chaque fois toutes ses prémisses (toutes les déclarations dans l'argument autre que la finale, la conclusion) sont vraies, la conclusion doit également être vraie.Supposons maintenant que les deux «Si vous avez un mot de passe actuel, vous pouvez vous connecter au réseau »et« Vous avez un mot de passe actuel »sont de véritables déclarations.Quand nous remplaçons p par «Vous avez un mot de passe actuel» et q par «Vous pouvez vous connecter au réseau», il s'ensuit nécessairement que la conclusion «Vous pouvez vous connecter au réseau» est vraie.Cet argument est **valide** car sa forme est valide. Notez que chaque fois que nous remplaçons p et q par des propositions où $p \to q$ et p sont tous deux vrais, alors q doit également être vrai.

Que se passe-t-il lorsque nous remplaçons p et q dans cette forme d'argument par des propositions où non à la fois p et $p \to q$ sont vraies? Par exemple, supposons que p représente «Vous avez accès au réseau "et q représente" Vous pouvez changer votre note "et que p est vrai, mais $p \to q$ est faux. L'argument que nous obtenons en substituant ces valeurs de p et q dans la forme d'argument est

"Si vous avez accès au réseau, vous pouvez modifier votre note."
"Vous avez accès au réseau."
$\therefore$ "Vous pouvez changer votre note."

L'argument que nous avons obtenu est un argument valide, mais parce que l'une des prémisses, à savoir le premier prémisse, est faux, nous ne pouvons pas conclure que la conclusion est vraie(Très probablement, cette conclusion c'est faux.)

Dans notre discussion, pour analyser un argument, nous avons remplacé les propositions par des variantes propositionnelles. aptes. Cela a changé un argument en une **forme d'argument** . Nous avons vu que la validité d'un argument découle de la validité de la forme de l'argument.Nous résumons la terminologie utilisée pour discuter de la validité des arguments avec notre définition des notions clés.

DÉFINITION 1 Un *argument* en logique propositionnelle est une séquence de propositions.Tout sauf la proposition finale dans l'argument sont appelés *prémisses* et la proposition finale est appelée la *conclusion* . Un L'argument est *valable* si la vérité de toutes ses prémisses implique que la conclusion est vraie.

Une *forme d'argument* dans la logique propositionnelle est une séquence de propositions composées des variables propositionnelles. Une forme d'argument est *valable* quelle que soit la proposition substitutions aux variables propositionnelles dans ses locaux, la conclusion est vraie si les prémisses sont toutes vraies.

De la définition d'une forme d'argument valide, nous voyons que la forme d'argument avec des prémisses $p_1, p_2, \ldots, p_n$ et la conclusion q est valide, lorsque $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ est une tautologie.

La clé pour montrer qu'un argument dans la logique propositionnelle est valide est de montrer que son la forme d'argument est valide. Par conséquent, nous aimerions que les techniques montrent que les formes d'argument sont valides. Nous allons maintenant développer des méthodes pour accomplir cette tâche.

Règles d'inférence pour la logique propositionnelle

Nous pouvons toujours utiliser une table de vérité pour montrer qu'une forme d'argument est valide.Nous le faisons en montrant que chaque fois que les prémisses sont vraies, la conclusion doit également être vraie.Cependant, cela peut être une approche fastidieuse. Par exemple, lorsqu'une forme d'argument implique 10 propositions différentes variables, pour utiliser une table de vérité pour montrer que cette forme d'argument est valide nécessite $2^{10} = 1024$ différents Lignes. Heureusement, nous n'avons pas à recourir à des tables de vérité.Au lieu de cela, nous pouvons d'abord établir la validité de certaines formes d'arguments relativement simples, appelées **règles d'inférence** . Ces règles de l'inférence peut être utilisée comme blocs de construction pour construire des formes d'arguments valides plus compliquées. Nous allons maintenant introduire les règles d'inférence les plus importantes dans la logique propositionnelle.

La tautologie $(p \wedge (p \to q)) \to q$ est la base de la règle d'inférence appelée **modus ponens** , ou la **loi du détachement** . (Modus ponens est latin pour le *mode qui affirme* .) Cette tautologie conduit à la forme d'argument valide suivante, que nous avons déjà vu dans notre discussion initiale sur les arguments (où, comme précédemment, le symbole $\therefore$ signifie "donc"):

p
$p \to q$
$\therefore q$

En utilisant cette notation, les hypothèses sont écrites dans une colonne, suivie d'une barre horizontale, suivie par une ligne qui commence par le symbole donc et se termine par la conclusion. En particulier, modus ponens nous dit que si une déclaration conditionnelle et l'hypothèse de cette déclaration conditionnelle sont à la fois vrai, alors la conclusion doit également être vraieL'exemple 1 illustre l'utilisation de modus ponens.

EXEMPLE 1 Supposons que l'énoncé conditionnel «S'il neige aujourd'hui, alors nous irons skier» et son l'hypothèse «Il neige aujourd'hui» est vraie. Ensuite, par modus ponens, il s'ensuit que la conclusion de l'énoncé conditionnel «Nous irons skier» est vrai. ▲

Comme nous l'avons mentionné précédemment, un argument valide peut conduire à une conclusion incorrecte si un ou plusieurs de ses prémisses sont fausses. Nous illustrons cela à nouveau dans l'exemple 2.

EXEMPLE 2 Déterminer si l'argument donné ici est valide et déterminer si sa conclusion doit être vrai en raison de la validité de l'argument.

"Si $\sqrt{2} > \frac{3}{2}$, puis $(\sqrt{2})^2 > (\frac{3}{2})^2$. Nous savons que $\sqrt{2} > \frac{3}{2}$. Par conséquent, $(\sqrt{2})^2 = 2 > (\frac{3}{2})^2 = \frac{9}{4}$."

Solution: Soit p la proposition "$\sqrt{2} > \frac{3}{2}$" »Et q la proposition« $2 > (\frac{3}{2})^2$. »Les locaux de l'argument sont $p \to q$ et p, et q est sa conclusion. Cet argument est valide car il est construit en utilisant modus ponens, une forme d'argument valide. Cependant, l'un de ses locaux, $\sqrt{2} > \frac{3}{2}$, c'est faux. Par conséquent, nous ne pouvons pas conclure que la conclusion est vraie. En outre, noter que la conclusion de cet argument est fausse, car $2 < \frac{9}{4}$. ▲

Il existe de nombreuses règles d'inférence utiles pour la logique propositionnelle. Peut-être le plus largement sont utilisées dans le tableau 1. Les exercices 9, 10, 15 et 30 de la section 1.3 demandent vérifie que ces règles d'inférence sont des formes d'argument valides. Nous donnons maintenant des exemples de des arguments qui utilisent ces règles d'inférence. Dans chaque argument, nous utilisons d'abord des variables propositionnelles pour exprimer les propositions dans l'argument. Nous montrons ensuite que la forme d'argument résultante est une règle d'inférence du tableau 1.

TABLEAU 1 **Règles d'inférence.**

Règle d'inférence	*Tautologie*	*Nom*
p $p \to q$ $\therefore q$	$(p \land (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \land (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Syllogisme hypothétique
$p \lor q$ $\neg p$ $\therefore q$	$((p \lor q) \land \neg p) \to q$	Syllogisme disjonctif
p $\therefore p \lor q$	$p \to (p \lor q)$	Une addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplification
p q $\therefore p \land q$	$((p) \land (q)) \to (p \land q)$	Conjonction
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Résolution

EXEMPLE 3 Indiquer quelle règle d'inférence est à la base de l'argument suivant: «Il est maintenant en dessous du gel. Par conséquent, il est en dessous de zéro ou il pleut maintenant. »

Solution: Soit p la proposition «Il fait maintenant moins de zéro maintenant» et q la proposition «Il pleut maintenant. "Alors cet argument est de la forme

$$\begin{array}{l} p \\ \therefore p \vee q \end{array}$$

Il s'agit d'un argument qui utilise la règle d'addition. ▲

EXEMPLE 4 Indiquer quelle règle d'inférence est à la base de l'argument suivant: «Elle est inférieure au gel et il pleut maintenant. Par conséquent, il est en dessous de zéro maintenant. »

Solution: Soit p la proposition «Il est en dessous de zéro maintenant» et q soit la proposition «C'est il pleut maintenant. »Cet argument est de la forme

$$\begin{array}{l} p \wedge q \\ \therefore p \end{array}$$

Cet argument utilise la règle de simplification. ▲

EXEMPLE 5 Indiquez quelle règle d'inférence est utilisée dans l'argument:

S'il pleut aujourd'hui, nous n'aurons pas de barbecue aujourd'hui. Si nous n'avons pas de barbecue aujourd'hui, alors nous aurons un barbecue demain. Par conséquent, s'il pleut aujourd'hui, nous aurons un barbecue demain.

Solution: Soit p la proposition «Il pleut aujourd'hui», soit q la proposition «Nous ne faire un barbecue aujourd'hui », et que r soit la proposition« Nous aurons un barbecue demain. »Ensuite cet argument est de la forme

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \therefore p \rightarrow r \end{array}$$

Par conséquent, cet argument est un syllogisme hypothétique. ▲

Utilisation de règles d'inférence pour créer des arguments

Lorsqu'il existe de nombreuses prémisses, plusieurs règles d'inférence sont souvent nécessaires pour montrer qu'un l'argument est valide. Ceci est illustré par les exemples 6 et 7, où les étapes des arguments sont affiché sur des lignes séparées, avec la raison de chaque étape explicitement indiquée. Ces exemples montrer comment les arguments en anglais peuvent être analysés à l'aide de règles d'inférence.

EXEMPLE 6 Montrer que les locaux «Il ne fait pas beau cet après-midi et il fait plus froid qu'hier», «Nous allons nager seulement s'il fait beau, "" Si nous ne nageons pas, alors nous ferons une excursion en canoë, " et "Si nous faisons un voyage en canoë, nous serons chez nous au coucher du soleil" conduisent à la conclusion "Nous être à la maison au coucher du soleil. "

Solution: Soit p la proposition «Il fait beau cet après-midi», q la proposition «Il fait plus froid que hier, » r la proposition « Nous allons nager, » *est* la proposition « Nous prendrons une Excursion en canot » , et t la proposition « Nous allons à lamaison par le coucher du soleil. » Ensuite , les locaux deviennent $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$ et $s \rightarrow t$. La conclusion est simplement t . Nous devons donner un valide argument avec prémisses $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$ et $s \rightarrow t$ et conclusion t .

Nous construisons un argument pour montrer que nos locaux conduisent à la conclusion souhaitée suit.

Étape	**Raison**
1. $\neg p \wedge q$	Prémisse
2. $\neg p$	Simplification avec (1)
3. $r \rightarrow p$	Prémisse
4. $\neg r$	Modus tollens utilisant (2) et (3)
5. $\neg r \rightarrow s$	Prémisse
6. s	Modus ponens utilisant (4) et (5)
7. $s \rightarrow t$	Prémisse
8. t	Modus ponens utilisant (6) et (7)

Notez que nous aurions pu utiliser une table de vérité pour montrer que chaque fois que chacune des quatre hypothèses est vrai, la conclusion est également vraie.Cependant, parce que nous travaillons avec cinq propositions variables, p , q , r , s et t , une telle table de vérité aurait 32 lignes. ▲

EXEMPLE 7 Montrez que les locaux «Si vous m'envoyez un e-mail, alors je finirai d'écrire le programme "," Si vous ne m'envoyez pas d'e-mail, je vais me coucher tôt "et" Si je m'en vais dormir tôt, puis je me réveillerai en me sentant rafraîchi »mène à la conclusion« Si je ne finis pas en écrivant le programme, je me réveillerai en me sentant rafraîchi. »

Solution: Soit p la proposition «Vous m'envoyez un e-mail», q la proposition «Je vais terminer l' écriture du programme, » r la proposition « Je vais aller dormir tôt » et s la proposition « I va se réveiller en se sentant rafraîchi. »Ensuite, les prémisses sont $p \to q$, $\neg p \to r$ et $r \to s$. La souhaitée la conclusion est $\neg q \to s$. Nous devons donner un argument valide avec les prémisses $p \to q$, $\neg p \to r$, et $r \to s$ et conclusion $\neg q \to s$.

Cette forme d'argument montre que les prémisses conduisent à la conclusion souhaitée.

Étape	**Raison**
1. $p \to q$	Prémisse
2. $\neg q \to \neg p$	Contrapositif de (1)
3. $\neg p \to r$	Prémisse
4. $\neg q \to r$	Syllogisme hypothétique utilisant (2) et (3)
5. $r \to s$	Prémisse
6. $\neg q \to s$	Syllogisme hypothétique utilisant (4) et (5)

▲

Résolution

Des programmes informatiques ont été développés pour automatiser la tâche de raisonnement et de démonstration rems. Beaucoup de ces programmes utilisent une règle d'inférence connue sous le nom de **résolution** . Cette règle de l'inférence est basée sur la tautologie

$$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r).$$

(L'exercice 30 de la section 1.3 demande de vérifier qu'il s'agit d'une tautologie.) La disjonction finale dans la règle de résolution, $q \vee r$, est appelée **résolvante** . Quand on laisse $q = r$ dans cette tautologie, on obtient $(p \vee q) \wedge (\neg p \vee q) \to q$. De plus, quand on laisse $r = \mathbf{F}$, on obtient $(p \vee q) \wedge (\neg p) \to q$ (car $q \vee \mathbf{F} \equiv q)$, qui est la tautologie sur laquelle se fonde la règle du syllogisme disjonctif.

EXEMPLE 8 Utilisez la résolution pour montrer que les hypothèses «Jasmine skie ou ne neige pas» et «Il est neige ou Bart joue au hockey »impliquent que« Jasmine fait du ski ou Bart joue au hockey. »

Solution: Soit p la proposition «Il neige», q la proposition «Jasmine fait du ski» et r la proposition «Bart joue au hockey». Nous pouvons représenter les hypothèses comme $\neg p \vee q$ et $p \vee r$, respectivement. En utilisant la résolution, la proposition $q \vee r$, «Jasmine skie ou Bart joue hockey », suit. ▲

La résolution joue un rôle important dans les langages de programmation basés sur les règles de la logique, comme Prolog (où les règles de résolution pour les états quantifiés sont appliquées).En outre, il peut être utilisé pour construire des systèmes de démonstration automatique de théorèmes.Construire des preuves en propositionnel la logique utilisant la résolution comme seule règle d'inférence, les hypothèses et la conclusion doivent être exprimé en **clauses** , où une clause est une disjonction de variables ou des négations de ces variables. On peut remplacer une déclaration en logique propositionnelle qui n'est pas une clause par un ou plusieurs équivalents déclarations qui sont des clauses. Par exemple, supposons que nous ayons une déclaration de la forme $p \vee (q \wedge r)$. Parce que $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, nous pouvons remplacer l'énoncé unique $p \vee (q \wedge r)$ par deux déclarations $p \vee q$ et $p \vee r$, chacune étant une clause. Nous pouvons remplacer une déclaration de la forme $\neg(p \vee q)$ par les deux énoncés $\neg p$ et $\neg q$ car la loi de De Morgan nous dit que $\neg(p \vee q) \equiv \neg p \wedge \neg q$. On peut aussi remplacer une instruction conditionnelle $p \to q$ par l'équivalent disjonction $\neg p \vee q$.

EXEMPLE 9 Montrer que les prémisses $(p \wedge q) \vee r$ et $r \rightarrow s$ impliquent la conclusion $p \vee s$.

Solution: On peut réécrire les prémisses $(p \wedge q) \vee r$ en deux clauses, $p \vee r$ et $q \vee r$. Nous pouvons aussi remplacer $r \rightarrow s$ par la clause équivalente $\neg r \vee s$. En utilisant les deux clauses $p \vee r$ et $\neg r \vee s$, nous pouvons utilisez la résolution pour conclure $p \vee s$. ▲

Fallacies

Plusieurs erreurs courantes surviennent dans des arguments incorrects. Ces erreurs ressemblent à des règles mais reposent sur des imprévus plutôt que sur des tautologies. Ceux-ci sont discutés ici pour montrer la distinction entre un raisonnement correct et incorrect.

La proposition $((p \rightarrow q) \wedge q) \rightarrow p$ n'est pas une tautologie, car elle est fausse quand p est fausse et q est vrai. Cependant, il existe de nombreux arguments incorrects qui traitent cela comme une tautologie. Dans en d'autres termes, ils traitent l'argument avec les prémisses $p \rightarrow q$ et q et la conclusion p comme valide forme d'argument, ce qui n'est pas le cas. Ce type de raisonnement incorrect est appelé l'**erreur d'affirmer la conclusion**.

EXEMPLE 10 L'argument suivant est-il valide?

Si vous faites tous les problèmes de ce livre, vous apprendrez des mathématiques discrètes. Tu as appris Mathématiques discrètes.

Par conséquent, vous avez fait tous les problèmes de ce livre.

Solution: Soit p la proposition «Vous avez fait tous les problèmes de ce livre». Soit q la proposition "Vous avez appris les mathématiques discrètes." Alors cet argument est de la forme: si $p \rightarrow q$ et q, alors p. Ceci est un exemple d'argument incorrect utilisant l'erreur de confirmer la conclusion.

En effet, il vous est possible d'apprendre des mathématiques discrètes autrement qu'en faisant tous les problème dans ce livre. (Vous pouvez apprendre des mathématiques discrètes en lisant, en écoutant des conférences, faire certains, mais pas tous, les problèmes de ce livre, etc.) ▲

La proposition $((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$ n'est pas une tautologie, car elle est fausse lorsque p est false et q est vrai. De nombreux arguments incorrects l'utilisent incorrectement comme règle d'inférence. Cette type de raisonnement incorrect est appelé l'**erreur de nier l'hypothèse**.

EXEMPLE 11 Soit p et q comme dans l'exemple 10. Si l'instruction conditionnelle $p \rightarrow q$ est vraie, et $\neg p$ est vraie, est-il correct de conclure que $\neg q$ est vrai? En d'autres termes, est-il correct de supposer que vous n'avez pas apprendre des mathématiques discrètes si vous n'avez pas fait tous les problèmes du livre, en supposant que si vous le faites chaque problème dans ce livre, alors vous apprendrez des mathématiques discrètes?

Solution: Il est possible que vous ayez appris des mathématiques discrètes même si vous n'avez pas fait tous les problème dans ce livre. Cet argument incorrect est de la forme $p \rightarrow q$ et $\neg p$ implique $\neg q$, qui est un exemple de l'erreur de nier l'hypothèse. ▲

Règles d'inférence pour les déclarations quantifiées

Nous avons discuté des règles d'inférence pour les propositions. Nous allons maintenant décrire quelques règles importantes d'inférence pour les déclarations impliquant des quantificateurs. Ces règles d'inférence sont largement utilisées dans les arguments mathématiques, souvent sans être explicitement mentionné.

L'instanciation universelle est la règle d'inférence utilisée pour conclure que $P(c)$ est vrai, où c est un membre particulier du domaine, étant donné la prémisse $\forall x P(x)$. L'instanciation universelle est utilisée quand nous concluons de la déclaration «Toutes les femmes sont sages» que «Lisa est sage», où Lisa est un membre du domaine de toutes les femmes.

TABLEAU 2 **Règles d'inférence pour les états quantifiés.**

Règle d'inférence	*Nom*
$\forall xP(x)$ $\therefore P(c)$	Instanciation universelle
$P(c)$ pour un c arbitraire $\therefore \forall xP(x)$	Généralisation universelle
$\exists xP(x)$ $\therefore P(c)$ pour un élément c	Instanciation existentielle
$P(c)$ pour un élément c $\therefore \exists xP(x)$	Généralisation existentielle

La généralisation universelle est la règle d'inférence qui stipule que $\forall xP(x)$ est vrai, étant donné la prémisse que $P(c)$ est vrai pour tous les éléments c dans le domaine. La généralisation universelle est utilisée lorsque nous montrons que $\forall xP(x)$ est vrai en prenant un élément arbitraire c du domaine et en montrant que $P(c)$ est vrai. L'élément c que nous sélectionnons doit être un élément arbitraire et non spécifique de le domaine. Autrement dit, lorsque nous affirmons à partir de $\forall xP(x)$ l'existence d'un élément c dans le domaine, nous n'avons aucun contrôle sur c et ne pouvons faire aucune autre hypothèse sur c autre que celle-ci du domaine. La généralisation universelle est implicitement utilisée dans de nombreuses preuves en mathématiques et est rarement mentionné explicitement. Cependant, l'erreur d'ajouter des hypothèses injustifiées l'élément arbitraire c lorsque la généralisation universelle est utilisée est trop courant dans incorrect raisonnement.

L'instanciation existentielle est la règle qui nous permet de conclure qu'il y a un élément c dans le domaine pour lequel $P(c)$ est vrai si l'on sait que $\exists xP(x)$ est vrai. Nous ne pouvons pas sélectionner un arbitraire valeur de c ici, mais plutôt ce doit être un c pour lequel $P(c)$ est vrai. Habituellement, nous n'avons aucune connaissance de ce que c est, seulement qu'il existe. Parce qu'il existe, nous pouvons lui donner un nom (c) et continuer notre argument.

La généralisation existentielle est la règle d'inférence utilisée pour conclure que $\exists xP(x)$ est vrai quand un élément particulier c avec $P(c)$ vrai est connu. Autrement dit, si nous connaissons un élément c dans le domaine pour lequel $P(c)$ est vrai, alors nous savons que $\exists xP(x)$ est vrai.

Nous résumons ces règles d'inférence dans le tableau 2. Nous allons illustrer comment certaines de ces règles d'inférence pour les énoncés quantifiés sont utilisés dans les exemples 12 et 13.

EXEMPLE 12 Montrer que les prémisses «Tout le monde dans ce cours de mathématiques discret a suivi un cours de informatique "et" Marla est étudiante dans cette classe "impliquent la conclusion" Marla a pris un cours d'informatique. "

Solution: Soit $D(x)$ dénoter « x est dans cette classe de mathématiques discrète», et soit $C(x)$ dénoter « x a suivi un cours d'informatique. »Ensuite, les locaux sont $\forall x(D(x) \rightarrow C(x))$ et D (Marla). La conclusion est C (Marla).

Les étapes suivantes peuvent être utilisées pour établir la conclusion à partir des locaux.

Étape	**Raison**
1. $\forall x(D(x) \rightarrow C(x))$	Prémisse
2. D (Marla) $\rightarrow C$ (Marla)	Instanciation universelle à partir de (1)
3. D (Marla)	Prémisse
4. C (Marla)	Modus ponens de (2) et (3)

▲

EXEMPLE 13 Montrer que les lieux «Un élève de cette classe n'a pas lu le livre» et «Tout le monde dans ce classe a réussi le premier examen "implique la conclusion" Quelqu'un qui a réussi le premier examen n'a pas lis le livre."

Solution: Soit $C(x)$ « x est dans cette classe», $B(x)$ soit « x a lu le livre», et $P(x)$ soit « x passé premier examen. »Les locaux sont $\exists x(C(x) \wedge \neg B(x))$ et $\forall x(C(x) \rightarrow P(x))$. La conclusion est $\exists x(P(x) \wedge \neg B(x))$. Ces étapes peuvent être utilisées pour établir la conclusion à partir des locaux.

Étape	**Raison**
1. $\exists x(C(x) \wedge \neg B(x))$	Prémisse
2. $C(a) \wedge \neg B(a)$	Instanciation existentielle de (1)
3. $C(a)$	Simplification à partir de (2)
4. $\forall x(C(x) \rightarrow P(x))$	Prémisse
5. $C(a) \rightarrow P(a)$	Instanciation universelle à partir de (4)
6. $P(a)$	Modus ponens de (3) et (5)
7. $\neg B(a)$	Simplification à partir de (2)
8. $P(a) \wedge \neg B(a)$	Conjonction de (6) et (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Généralisation existentielle de (8)

▲

Combiner les règles d'inférence pour les propositions et déclarations quantifiées

Nous avons développé des règles d'inférence tant pour les propositions que pour les énoncés quantifiésRemarque que dans nos arguments des exemples 12 et 13, nous avons utilisé à la fois l'instanciation universelle, une règle de l'inférence pour les énoncés quantifiés, et le modus ponens, une règle d'inférence pour la logique propositionnelle. Nous aurons souvent besoin d'utiliser cette combinaison de règles d'inférence.Parce que l'instanciation universelle et modus ponens sont utilisés si souvent ensemble, cette combinaison de règles est parfois appelée **modus ponens universel** . Cette règle nous dit que si $\forall x(P(x) \rightarrow Q(x))$ est vrai, et si $P(a)$ est vrai pour un élément particulier a dans le domaine du quantificateur universel, alors $Q(a)$ doit aussi Sois sincère. Pour voir cela, notons que par instanciation universelle, $P(a) \rightarrow Q(a)$ est vrai. Ensuite, par modus ponens, $Q(a)$ doit également être vrai.Nous pouvons décrire le modus ponens universel comme suit:

$\forall x(P(x) \rightarrow Q(x))$

$P(a)$, où a est un élément particulier du domaine

$\therefore Q(a)$

Le modus ponens universel est couramment utilisé dans les arguments mathématiques. Ceci est illustré dans l'exemple 14.

EXEMPLE 14 Supposons que «pour tous les entiers positifs n , si n est supérieur à 4, alors n^2 est inférieur à 2^n " est vrai. Utilisez des modus ponens universels pour montrer que $100^2 < 2^{100}$.

Solution: Soit $P(n)$ dénoter « $n > 4$» et $Q(n)$ dénoter « $n^2 < 2^n$ ». "La déclaration" Pour tous positifs entiers n , si n est supérieur à 4, alors n^2 est inférieur à 2^n »Peut être représenté par $\forall n(P(n) \rightarrow Q(n))$, où le domaine se compose de tous les entiers positifs. Nous supposons que $\forall n(P(n) \rightarrow Q(n))$ est vrai. Notez que $P(100)$ est vrai car $100 > 4$. Il s'ensuit par modus ponens universel que $Q(100)$ est vrai, à savoir que $100^2 < 2^{100}$. ▲

Une autre combinaison utile d'une règle d'inférence à partir de la logique propositionnelle et d'une règle d'inférence quantifiée est **le modus tollens universel** . Modus tollens universel

combine l'instanciation universelle et le modus tollens et peut s'exprimer de la manière suivante:

$\forall x(P(x) \rightarrow Q(x))$

$\neg Q(a)$, où a est un élément particulier du domaine

$\therefore \neg P(a)$

La vérification du modus tollens universel est laissée à l'exercice 25. Les exercices 26 à 29 développent combinaisons supplémentaires de règles d'inférence dans la logique propositionnelle et les énoncés quantifiés.

Des exercices

1. Recherchez la forme d'argument pour l'argument suivant et déterminer s'il est valide. Pouvons-nous conclure que le la conclusion est vraie si les prémisses sont vraies?

Si Socrate est humain, alors Socrate est mortel.
Socrate est humain.
∴ Socrate est mortel.

2. Recherchez la forme d'argument pour l'argument suivant et déterminer s'il est valide. Pouvons-nous conclure que le la conclusion est vraie si les prémisses sont vraies?

Si George n'a pas huit pattes, alors il n'est pas un araignée.
George est une araignée.
∴ George a huit pattes.

3. Quelle règle d'inférence est utilisée dans chacun de ces arguments ments?

a) Alice est majeure en mathématiques. Par conséquent, Alice est ei- il y a une majeure en mathématiques ou une majeure en informatique.

b) Jerry est majeur en mathématiques et en informatique Majeur. Par conséquent, Jerry est majeur en mathématiques.

c) S'il pleut, la piscine sera fermée. Il pleut. Par conséquent, la piscine est fermée.

d) S'il neige aujourd'hui, l'université fermera. L'uni- la versité n'est pas fermée aujourd'hui. Par conséquent, il n'a pas neigé aujourd'hui.

e) Si je vais nager, je resterai trop longtemps au soleil. Si je reste trop longtemps au soleil, je vais avoir des coups de soleil. Là- Par conséquent, si je vais nager, je prendrai un coup de soleil.

4. Quelle règle d'inférence est utilisée dans chacun de ces arguments?

a) Les kangourous vivent en Australie et sont des marsupiaux. Là- Par conséquent, les kangourous sont des marsupiaux.

b) Il fait plus chaud que 100 degrés aujourd'hui ou la pollution tion est dangereuse. Il fait moins de 100 degrés à l'extérieur aujourd'hui. Par conséquent, la pollution est dangereuse.

c) Linda est une excellente nageuse. Si Linda est une excellente nageuse, puis elle peut travailler comme sauveteur. Donc, Linda peut travailler comme sauveteur.

d) Steve travaillera dans une entreprise informatique cet été. Par conséquent, cet été, Steve travaillera sur un ordinateur entreprise ou il sera un clochard de plage.

e) Si je travaille toute la nuit sur ces devoirs, alors je peux swer tous les exercices. Si je réponds à tous les exercices, je comprendra le matériel. Par conséquent, si je travaille tous nuit sur ces devoirs, alors je comprendrai la Matériel.

5. Utiliser des règles d'inférence pour montrer que les hypothèses «Randy travaille dur, "" Si Randy travaille dur, alors il est un garçon terne, " et "Si Randy est un garçon terne, alors il n'obtiendra pas le travail" impliquent la conclusion «Randy n'obtiendra pas le travail.»

6. Utilisez des règles d'inférence pour montrer que les hypothèses «Si ne pleut pas ou s'il ne fait pas de brouillard, la course de voile se tiendra et la démonstration de sauvetage continuera, "" Si la course de voile a lieu, puis le trophée sera décerné », et "Le trophée n'a pas été décerné" implique la conclusion "Il pleuvait."

7. Quelles règles d'inférence sont utilisées dans ce fameux argument ment? «Tous les hommes sont mortels. Socrate est un homme. Donc, Socrate est mortel. "

8. Quelles règles d'inférence sont utilisées dans cet argument? "Non l'homme est une île. Manhattan est une île. Par conséquent, Man- hattan n'est pas un homme. "

9. Pour chacune de ces collections de locaux, quels éléments conclusion ou des conclusions peuvent être tirées? Expliquer le règles d'inférence utilisées pour obtenir chaque conclusion les locaux.

a) "Si je prends un jour de congé, il pleut ou il neige." "J'ai pris Mardi ou j'ai pris jeudi. »« Il faisait beau Mardi. "" Il n'a pas neigé jeudi. "

b) "Si je mange des aliments épicés, alors j'ai des rêves étranges." "Je fais d'étranges rêves s'il y a du tonnerre pendant que je dors. » "Je n'ai pas fait de rêves étranges."

c) "Je suis intelligent ou chanceux." "Je n'ai pas de chance." "Si je j'ai de la chance, alors je gagnerai à la loterie. »

d) «Chaque spécialisation en informatique a une com- ordinateur. "" Ralph n'a pas d'ordinateur personnel. " "Ann a un ordinateur personnel."

e) «Ce qui est bon pour les sociétés est bon pour les États-Unis États-Unis. "" Ce qui est bon pour les États-Unis est bon pour vous. "" Ce qui est bon pour les entreprises, c'est que vous acheter beaucoup de choses. "

f) «Tous les rongeurs rongent leur nourriture.» «Les souris sont des rongeurs.» «Les lapins ne rongent pas leur nourriture.» «Les chauves-souris ne sont pas dents. "

10. Pour chacun de ces ensembles de locaux, quelles conclusions pertinentes sion ou des conclusions peuvent être tirées? Expliquez les règles de utilisé pour obtenir chaque conclusion des lieux.

a) «Si je joue au hockey, alors j'ai mal le lendemain.» «Je utiliser le bain à remous si j'ai mal. "" Je n'ai pas utilisé le tourbillon."

b) «Si je travaille, c'est ensoleillé ou partiellement ensoleillé.» «J'ai travaillé lundi dernier ou j'ai travaillé vendredi dernier. »« Il ne faisait pas beau mardi. "" Ce n'était pas partiellement ensoleillé vendredi. "

c) "Tous les insectes ont six pattes." "Les libellules sont des insectes." "Les araignées n'ont pas six pattes." "Les araignées mangent du dragon- mouches."

d) "Chaque élève a un compte Internet." "Homer ne pas de compte Internet. "" Maggie a un Internet Compte."

e) «Tous les aliments sains à manger n'ont pas bon goût.» «Le tofu est sain à manger.» «On ne mange que ce qui a le goût bon. "" Vous ne mangez pas de tofu. "" Les cheeseburgers ne sont pas sain à manger. "

b) «Chacun des cinq colocataires, Melissa, Aaron, Ralph, Ve- neesha et Keeshawn ont suivi un cours discret mathématiques. Chaque étudiant qui a suivi un cours en les mathématiques discrètes peuvent suivre un cours d'algorithmes. Par conséquent, les cinq colocataires peuvent suivre un cours de algorithmes l'année prochaine. "

c) «Tous les films produits par John Sayles sont ful. John Sayles a produit un film sur les mineurs de charbon. Par conséquent, il y a un merveilleux film sur les mines de charbon ers. "

d) «Il y a quelqu'un dans cette classe qui a été France. Tous ceux qui vont en France visitent le Persienne. Par conséquent, quelqu'un de cette classe a visité le Louvre."

15. Pour chacun de ces arguments, déterminez si l'argument ment est correct ou incorrect et expliquez pourquoi.

a) Tous les élèves de cette classe comprennent la logique. Xavier est un élève de cette classe. Par conséquent, Xavier comprend logique.

b) Chaque majeure en informatique requiert des mathématiques discrètes

f) «Je rêve ou hallucine.» «Je ne suis pas rêver. "" Si j'hallucine, je vois des éléphants courir sur la route. "

11. Montrer que la forme d'argument avec les locaux $p_1, p_2, \ldots, p_n$ et la conclusion $q \rightarrow r$ est valable si le forme d'argument avec les prémisses $p_1, p_2, \ldots, p_n, q$ et la conclusion r est valable.

12. Montrer que l'argument forme avec des prémisses $(p \wedge t) \rightarrow (r \vee s)$, $q \rightarrow (u \wedge t)$, $u \rightarrow p$, et $\neg s$ et conclusion $q \rightarrow r$ est valide en utilisant d'abord l'exercice 11 puis en utilisant règles d'inférence du tableau 1.

13. Pour chacun de ces arguments, expliquez quelles règles de la fermentation est utilisée pour chaque étape.

a) «Doug, un élève de cette classe, sait écrire programmes en JAVA. Tous ceux qui savent écrire les programmes de JAVA peuvent obtenir un emploi bien rémunéré. Là- Par conséquent, quelqu'un dans cette classe peut obtenir un emploi bien rémunéré. »

b) «Quelqu'un dans cette classe aime observer les baleines. Ev- Chaque personne qui aime observer les baleines se soucie pollution des océans. Par conséquent, il y a une personne dans ce classe qui se soucie de la pollution des océans. "

c) «Chacun des 93 élèves de cette classe possède un ordinateur. Quiconque possède un ordinateur personnel peut utiliser un programme de traitement de texte. Par conséquent, Zeke, un élève de cette classe, peut utiliser un pro- gramme."

d) «Tout le monde dans le New Jersey vit à moins de 50 miles de la océan. Quelqu'un dans le New Jersey n'a jamais vu océan. Par conséquent, quelqu'un qui vit à moins de 50 miles de l'océan n'a jamais vu l'océan. "

14. Pour chacun de ces arguments, expliquez quelles règles de la fermentation est utilisée pour chaque étape.

a) «Linda, une élève de cette classe, possède une décapotable rouge. Tous ceux qui possèdent un cabriolet rouge sont arrivés à au moins un excès de vitesse. Par conséquent, quelqu'un dans ce classe a obtenu un excès de vitesse. "

ématiques. Natasha prend des mathématiques discrètes. Par conséquent, Natasha est une majeure en informatique.

c) Tous les perroquets aiment les fruits. Mon oiseau de compagnie n'est pas un perroquet. Là- Par conséquent, mon oiseau de compagnie n'aime pas les fruits.

d) Tous ceux qui mangent du granola tous les jours sont en bonne santé. Linda n'est pas sain. Par conséquent, Linda ne mange pas de granola tous les jours.

16. Pour chacun de ces arguments, déterminez si l'argument ment est correct ou incorrect et expliquez pourquoi.

a) Toutes les personnes inscrites à l'université ont vécu dans un mitory. Mia n'a jamais vécu dans un dortoir. Donc, Mia n'est pas inscrite à l'université.

b) Une voiture décapotable est agréable à conduire. La voiture d'Isaac n'est pas convertible. Par conséquent, la voiture d'Isaac n'est pas agréable à conduire.

c) Quincy aime tous les films d'action. Quincy aime le film *Huit hommes dehors* . Par conséquent, *Eight Men Out* est une action film.

d) Tous les homardiers installent au moins une douzaine de pièges. Hamilton est un homard. Par conséquent, Hamilton définit au moins une douzaine pièges.

17. Quel est le problème avec cet argument? Soit $H(x)$ soit « x est heureux. "Étant donné la prémisse $\exists x H(x)$, nous concluons que H (Lola). Par conséquent, Lola est heureuse.

18. Quel est le problème avec cet argument? Soit $S(x, y)$ « x est plus court que y . »Étant donné la prémisse $\exists s S(s,$ Max), il s'ensuit que S (Max, Max). Ensuite, par généralisation existentielle, suit que $\exists x S(x, x)$, de sorte que quelqu'un est plus *petit* que lui-même.

19. Déterminez si chacun de ces arguments est valide. Si un l'argument est correct, quelle règle d'inférence est utilisée? Si ce n'est pas le cas, quelle erreur logique se produit?

a) Si n est un nombre réel tel que $n > 1$, alors $n^2 > 1$. Supposons que $n^2 > 1$. Alors $n > 1$.

b) Si n est un nombre réel avec $n > 3$, alors $n^2 > 9$. Supposons que $n^2 \leq 9$. Alors $n \leq 3$.

c) Si n est un nombre réel avec $n > 2$, alors $n^2 > 4$. Supposons que $n \leq 2$. Alors $n^2 \leq 4$.

20. Déterminez s'il s'agit d'arguments valides.

a) Si x est un nombre réel positif, alors x^2 est un réel positif nombre. Par conséquent, si un^2 est positif, où a est un réel nombre, alors a est un nombre réel positif.

b) Si $x^2 = 0$, où x est un nombre réel, alors $x = 0$. Soit a être un nombre réel avec $un^2 = 0$; alors $a = 0$.

21. Quelles règles d'inférence sont utilisées pour établir le conclusion de l'argument de Lewis Carroll décrit dans Exemple 26 de la section 1.4?

22. Quelles règles d'inférence sont utilisées pour établir le conclusion de l'argument de Lewis Carroll décrit dans Exemple 27 de la section 1.4?

23. Identifiez l'erreur ou les erreurs dans cet argument qui montre que si $\exists x P(x) \wedge \exists x Q(x)$ est vrai alors $\exists x (P(x) \wedge Q(x))$ est vrai.

1. $\exists x P(x) \vee \exists x Q(x)$ Local	
2. $\exists x P(x)$	Simplification à partir de (1)
3. $P(c)$	Instanciation existentielle de (2)
4. $\exists x Q(x)$	Simplification à partir de (1)
5. $Q(c)$	Instanciation existentielle de (4)
6. $P(c) \wedge Q(c)$	Conjonction de (3) et (5)
7. $\exists x (P(x) \wedge Q(x))$	Généralisation existentielle

24. Identifiez l'erreur ou les erreurs dans cet argument qui montre que si $\forall x (P(x) \vee Q(x))$ est vrai, alors $\forall x P(x) \vee \forall x Q(x)$ est vrai.

1. $\forall x (P(x) \vee Q(x))$	Prémisse
2. $P(c) \vee Q(c)$	Instanciation universelle à partir de (1)
3. $P(c)$	Simplification à partir de (2)
4. $\forall x P(x)$	Généralisation universelle à partir de (3)
5. $Q(c)$	Simplification à partir de (2)
6. $\forall x Q(x)$	Généralisation universelle à partir de (5)
7. $\forall x (P(x) \vee \forall x Q(x))$ Conjonction de (4) et (6)	

25. Justifiez la règle du modus tollens universel en montrant que les prémisses $\forall x (P(x) \rightarrow Q(x))$ et $\neg Q(a)$ pour un élément particulier a dans le domaine, implique $\neg P(a)$.

29. Utiliser des règles d'inférence pour montrer que si $\forall x (P(x) \vee Q(x))$, $\forall x (\neg Q(x) \vee S(x))$, $\forall x (R(x) \rightarrow \neg S(x))$ et $\exists x \neg P(x)$ sont vrais, alors $\exists x \neg R(x)$ est vrai.

30. Utilisez la résolution pour montrer les hypothèses «Allen est un mauvais garçon ou Hillary est une bonne fille "et" Allen est un bon garçon ou David est heureux "implique la conclusion" Hillary est une bonne fille ou David est heureux. "

31. Utilisez la résolution pour montrer que les hypothèses «Ce n'est pas ou Yvette a son parapluie, "" Yvette n'a pas son parapluie ou elle ne se mouille pas »et« Il pleut ou Yvette ne se mouille pas "implique que" Yvette ne se mouiller. "

32. Montrer que l'équivalence $p \wedge \neg p \equiv \mathbf{F}$ peut être dérivée en utilisant la résolution ainsi que le fait qu'une condition La déclaration provisoire avec une fausse hypothèse est vraie. [*Indice:* laissez $q = r = \mathbf{F}$ en résolution.]

33. Utilisez la résolution pour montrer que le composé proposé sition $(p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$ est pas satisfaisable.

∗ **34.** The Logic Problem, tiré de *WFF'N PROOF, The Game of Logic* , a ces deux hypothèses:

1 . "La logique est difficile ou peu d'étudiants aiment la logique."
2 . "Si les mathématiques sont faciles, alors la logique n'est pas difficile."

En traduisant ces hypothèses en déclarations impliquant des variables propositionnelles et des connecteurs logiques, déterminer si chacune des conclusions suivantes est valide de ces hypothèses:

a) Que les mathématiques ne sont pas faciles, si de nombreux élèves aiment logique.

b) Que peu d'élèves aiment la logique, si les mathématiques sont pas facile.

c) Que les mathématiques ne sont pas faciles ou que la logique est difficile.

d) Cette logique n'est pas difficile ou les mathématiques ne sont pas faciles.

26. Justifiez la règle de **la transitivité universelle** , qui stipule que si $\forall x (P(x) \to Q(x))$ et $\forall x (Q(x) \to R(x))$ sont vrais, alors $\forall x (P(x) \to R(x))$ est vrai, où les domaines de tous les quantificateurs sont les mêmes.

27. Utiliser des règles d'inférence pour montrer que si $\forall x (P(x) \to (Q(x) \wedge S(x)))$ et $\forall x (P(x) \wedge R(x))$ sont vrais, alors $\forall x (R(x) \wedge S(x))$ est vrai.

28. Utiliser des règles d'inférence pour montrer que si $\forall x (P(x) \vee Q(x))$ et $\forall x ((\neg P(x) \wedge Q(x)) \to R(x))$ sont vrais, alors $\forall x (\neg R(x) \to P(x))$ est également vrai, où les domaines de tous les quantificateurs sont identiques.

e) Que si peu d'élèves aiment la logique, alors soit les mathématiques rématique n'est pas facile ou la logique n'est pas difficile.

∗ **35.** Déterminez si cet argument, tiré de Kalish et Montague [KaMo64], est valide.

Si Superman était capable et désireux d'empêcher le mal, il le ferait. Si Superman était incapable d'empêcher mauvais, il serait impuissant; s'il ne voulait pas pour empêcher le mal, il serait malveillant. Superman n'empêche pas le mal. Si Superman existe, il n'est là impuissant ni malveillant. Par conséquent, Superman n'existe pas.

Introduction aux preuves

introduction

Dans cette section, nous introduisons la notion de preuve et décrivons les méthodes de construction des preuves. Une preuve est un argument valable qui établit la vérité d'une affirmation mathématique.Une preuve peut utiliser les hypothèses du théorème, le cas échéant, des axiomes supposés vrais, et prouvés précédemment

théorèmes. En utilisant ces ingrédients et règles d'inférence, la dernière étape de la preuve établit la vérité de la déclaration étant prouvée.

Dans notre discussion, nous passons de preuves formelles de théorèmes à des preuves plus informelles. Les arguments que nous avons introduits dans la section 1.6 pour montrer que les déclarations impliquant des propositions et les déclarations quantifiées sont vraies étaient des preuves formelles, où toutes les étapes ont été fournies, et la des règles pour chaque étape de l'argument ont été données.Cependant, des preuves formelles de théorèmes utiles peuvent être extrêmement long et difficile à suivre.En pratique, les preuves de théorèmes conçus pour l'homme la consommation sont presque toujours **des preuves informelles** , où plus d'une règle d'inférence peut être utilisé à chaque étape, où les étapes peuvent être sautées, où les axiomes étant supposés et les les règles d'inférence utilisées ne sont pas explicitement énoncées.Les preuves informelles peuvent souvent expliquer aux humains pourquoi les théorèmes sont vrais, alors que les ordinateurs sont parfaitement heureux de produire des preuves formelles en utilisant systèmes de raisonnement automatisés.

Les méthodes de preuve discutées dans ce chapitre sont importantes non seulement parce qu'elles sont utilisées pour prouver les théorèmes mathématiques, mais aussi pour leurs nombreuses applications à l'informatique.Celles-ci les applications comprennent la vérification de l'exactitude des programmes informatiques, l'établissement de les systèmes sont sécurisés, ce qui permet de tirer des conclusions en intelligence artificielle, montrant que les sont cohérentes, etc. Par conséquent, comprendre les techniques utilisées dans les preuves est essentiel à la fois en mathématiques et en informatique.

Quelques terminologies

Formellement, un **théorème** est une affirmation qui peut être vérifiée.En écriture mathématique, le théorème des termes est généralement réservé à une déclaration considérée au moins comme quelque peu importante. Les théorèmes moins importants sont parfois appelés **propositions** . (On peut également se référer aux théorèmes comme des **faits** ou des **résultats** .) Un théorème peut être la quantification universelle d'une déclaration conditionnelle avec un ou plusieurs prémisses et une conclusion. Cependant, il peut s'agir d'un autre type de logique , comme le montrent les exemples plus loin dans ce chapitre.Nous démontrons qu'un théorème est vrai avec une **preuve** . Une preuve est un argument valable qui établit la vérité d'un théorème. Les déclarations utilisé dans une preuve peut inclure des **axiomes** (ou **postulats**), qui sont des déclarations que nous supposons être vraies (par exemple, les axiomes des nombres réels, donnés à l'annexe 1, et les axiomes du plan géométrie), les prémisses, le cas échéant, du théorème, et les théorèmes précédemment prouvés.Les axiomes peuvent être énoncé en utilisant des termes primitifs qui ne nécessitent pas de définition, mais tous les autres termes utilisés dans les théorèmes et leurs preuves doivent être définies.Des règles d'inférence, ainsi que des définitions de termes, sont utilisées tirer des conclusions d'autres affirmations, en liant ensemble les étapes d'une preuve.En pratique, le l'étape finale d'une preuve n'est généralement que la conclusion du théorème.Cependant, pour plus de clarté, nous récapitule souvent l'énoncé du théorème comme la dernière étape d'une preuve.

Un théorème moins important qui est utile pour la preuve d'autres résultats est appelé un **lemme** (pluriel *lemmes* ou *lemmes*). Les preuves compliquées sont généralement plus faciles à comprendre lorsqu'elles sont prouvé en utilisant une série de lemmes, où chaque lemme est prouvé individuellement.Un **corollaire** est un théorème qui peut être établi directement à partir d'un théorème qui a été prouvé.Une **conjecture** est une déclaration qui est proposée pour être une véritable déclaration, généralement sur la base de certaines des preuves, un argument heuristique ou l'intuition d'un expert. Lorsqu'une preuve d'une conjecture est trouvée, la conjecture devient un théorème. Plusieurs fois, les conjectures se révèlent fausses, elles ne sont pas des théorèmes.

Comprendre comment les théorèmes sont énoncés

Avant d'introduire des méthodes pour prouver des théorèmes, nous devons comprendre combien de les théorèmes ématiques sont énoncés. De nombreux théorèmes affirment qu'une propriété vaut pour tous les éléments un domaine, comme les entiers ou les nombres réels. Bien que la déclaration précise de ces

les théorèmes doivent inclure un quantificateur universel, la convention standard en mathématiques est de omettez-le. Par exemple, la déclaration

"Si $x > y$, où x et y sont des nombres réels positifs, alors $x^2 > y^2$. "

signifie vraiment

"Pour tous les nombres réels positifs x et y , si $x > y$, alors $x^2 > y^2$. "

De plus, lorsque des théorèmes de ce type sont prouvés, la première étape de la démonstration implique généralement sélection d'un élément général du domaine. Les étapes suivantes montrent que cet élément a le propriété en question. Enfin, la généralisation universelle implique que le théorème est valable pour tous membres du domaine.

Méthodes de démonstration des théorèmes

Il peut être difficile de prouver des théorèmes mathématiques. Pour construire des preuves, nous avons besoin de toutes les munitions, y compris une batterie puissante de différentes méthodes de preuve. Ces méthodes fournissent approche globale et stratégie des preuves. La compréhension de ces méthodes est un élément clé de apprendre à lire et à construire des preuves mathématiques. Nous avons choisi une méthode de preuve, nous utilisons des axiomes, des définitions de termes, des résultats précédemment prouvés et des règles d'inférence pour compléter la preuve. Notez que dans ce livre, nous supposerons toujours les axiomes pour les nombres réels que l'on trouve à l'annexe 1. Nous supposerons également les axiomes habituels chaque fois que nous prouverons géométrie. Lorsque vous construisez vos propres preuves, veillez à ne pas utiliser autre chose que ces axiomes, définitions, et les résultats précédemment prouvés comme faits!

Pour prouver un théorème de la forme $\forall x\ (P(x) \rightarrow Q(x))$, notre objectif est de montrer que $P(c) \rightarrow Q(c)$ est vrai, où c est un élément arbitraire du domaine, puis applique la généralisation universelle. Dans cette preuve, nous devons montrer qu'une déclaration conditionnelle est vraie. Pour cette raison, nous nous concentrons maintenant sur les méthodes qui montrent que les déclarations conditionnelles sont vraies. Rappelons que $p \rightarrow q$ est vrai sauf si p est vrai mais q est faux. Notez que pour prouver l'énoncé $p \rightarrow q$, il suffit de montrer que q est vrai si p est vrai. La discussion suivante donnera les techniques les plus courantes pour prouver le conditionnel déclarations. Plus tard, nous discuterons des méthodes pour prouver d'autres types de déclarations. Dans cette section, et dans la section 1.8, nous développerons un large arsenal de techniques de preuve qui peuvent être utilisées pour prouver une grande variété de théorèmes.

Lorsque vous lisez des épreuves, vous trouverez souvent les mots «évidemment» ou «clairement». Ces mots indiquent que des étapes ont été omises et que l'auteur s'attend à ce que le lecteur puisse les remplir. Malheureusement, cette hypothèse n'est souvent pas justifiée et les lecteurs ne savent pas du tout comment remplir les trous. Nous essaierons assidûment d'éviter d'utiliser ces mots et de ne pas omettre trop d'étapes. Cependant, si nous incluions toutes les étapes dans les épreuves, nos épreuves seraient souvent d'une durée atroce.

Preuves directes

Une **preuve directe** d'une instruction conditionnelle $p \rightarrow q$ est construite lorsque la première étape est la hypothèse que p est vrai; les étapes suivantes sont construites en utilisant des règles d'inférence, dernière étape montrant que q doit également être vrai. Une preuve directe montre qu'une déclaration conditionnelle $p \rightarrow q$ est vrai en montrant que si p est vrai, alors q doit aussi être vrai, de sorte que la combinaison p true et q false ne se produisent jamais. Dans une preuve directe, nous supposons que p est vrai et utilisons des axiomes, définitions et théorèmes précédemment prouvés, ainsi que des règles d'inférence, pour montrer que q Vous devez également constater que les preuves directes de nombreux résultats sont assez simples, avec une séquence d'étapes assez évidente menant de l'hypothèse à la conclusion. Cependant, les preuves nécessitent parfois des informations particulières et peuvent être assez délicates Les premières preuves directes que nous présents ici sont assez simples; plus loin dans le texte, vous en verrez des moins évidentes.

Nous fournirons des exemples de plusieurs preuves directes différentes. Avant de donner le premier exemple, nous devons définir une terminologie.

DÉFINITION 1 L'entier n est *pair* s'il existe un entier k tel que $n = 2k$, et n est *impair* s'il existe un entier k tel que $n = 2k + 1$. (Notez que chaque entier est pair ou impair, et aucun entier est à la fois pair et impair.) Deux entiers ont la *même parité* lorsque les deux sont pairs ou les deux sont étranges; ils ont *une parité opposée* lorsque l'un est pair et l'autre impair.

EXEMPLE 1 Donner une preuve directe du théorème "Si n est un entier impair, alors n^2 est impair."

Solution: Notez que ce théorème énonce $\forall n P((n) \to Q(n))$, où $P(n)$ est « n est un entier impair» et $Q(n)$ est « n^2 est impair». Comme nous l'avons dit, nous suivrons la convention habituelle en mathématiques preuves en montrant que $P(n)$ implique $Q(n)$, et en n'utilisant pas explicitement l'instanciation universelle. À commencer une preuve directe de ce théorème, nous supposons que l'hypothèse de cette déclaration conditionnelle est vrai, à savoir, nous supposons que n est impair. Par la définition d'un entier impair, il s'ensuit que $n = 2k + 1$, où k est un entier. Nous voulons montrer que n^2 est également impair. Nous pouvons cadrer les deux côtés de l'équation $n = 2k + 1$ pour obtenir une nouvelle équation qui exprime n^2. Quand on fait cela, nous constatons que $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Par la définition d'un entier impair, nous pouvons conclure que n^2 est un entier impair (c'est un plus de deux fois un entier). Par conséquent, nous avons prouvé que si n est un entier impair, alors n^2 est un entier impair. ▲

EXEMPLE 2 Donner une preuve directe que si m et n sont tous les deux des carrés parfaits, alors nm est également un carré parfait. (Un entier a est un **carré parfait** s'il y a un entier b tel que $a = b^2$.)

Solution: Pour produire une preuve directe de ce théorème, nous supposons que l'hypothèse de cette l'énoncé conditionnel est vrai, à savoir, nous supposons que m et n sont tous les deux des carrés parfaits. Par le définition d'un carré parfait, il s'ensuit qu'il existe des entiers s et t tels que $m = s^2$ et $n = t^2$. Le but de la preuve est de montrer que mn doit aussi être un carré parfait quand m et n *le* sont; à l'avenir, nous voyons comment nous pouvons le montrer en remplaçant s^2 par m et t^2 par n en mn. Cette nous dit que $mn = s^2 t^2$. Donc, $mn = s^2 t^2 = (ss)(tt) = (st)(st) = (st)^2$, en utilisant la commutativité et associativité de la multiplication. Par la définition du carré parfait, il s'ensuit que mn est également un carré parfait, car c'est le carré de st, qui est un entier. Nous avons prouvé que si m et n sont tous les deux des carrés parfaits, alors mn est également un carré parfait. ▲

Preuve par contreposition

Les preuves directes mènent des prémisses d'un théorème à la conclusion. Ils commencent par le locaux, continuez avec une séquence de déductions et terminez par la conclusion. Toutefois, nous verront que les tentatives de preuves directes atteignent souvent des impasses. Nous avons besoin d'autres méthodes pour prouver théorèmes de la forme $\forall x(P(x) \to Q(x))$. Preuves de théorèmes de ce type qui ne sont pas directs les preuves, c'est-à-dire qui ne commencent pas par les prémisses et se terminent par la conclusion, sont appelées **preuves indirectes**.

Un type de preuve indirecte extrêmement utile est connu sous le nom de **preuve par contraposition**. Preuves par contraposition, utiliser le fait que l'énoncé conditionnel $p \to q$ est équivalent à son contrapositif, $\neg q \to \neg p$. Cela signifie que l'énoncé conditionnel $p \to q$ peut être démontré par montrant que sa contrapositive, $\neg q \to \neg p$, est vraie. Dans une preuve par contraposition de $p \to q$, nous prendre $\neg q$ comme prémisse, et en utilisant des axiomes, des définitions et des théorèmes déjà prouvés, ensemble avec des règles d'inférence, nous montrons que $\neg p$ doit suivre. Nous illustrerons la preuve par contraposition avec deux exemples. Ces exemples montrent que la preuve par contraposition peut réussir lorsque nous ne peut pas facilement trouver une preuve directe.

EXEMPLE 3 Démontrer que si n est un entier et $3n + 2$ est impair, alors n est impair.

Solution: Nous essayons d'abord une preuve directe. Pour construire une preuve directe, nous supposons d'abord que $3n + 2$ est un entier impair. Cela signifie que $3n + 2 = 2k + 1$ pour un entier k. Pouvons-nous utiliser ce fait montrer que n est impair? On voit que $3n + 1 = 2k$, mais il ne semble pas y avoir de voie directe pour conclure que n est impair. Parce que notre tentative de preuve directe a échoué, nous essayons ensuite une preuve par contraposition.

La première étape d'une preuve par contraposition est de supposer que la conclusion de la conditionnelle la déclaration «Si $3n + 2$ est impair, alors n est impair» est fausse;à savoir, supposons que n est pair. Puis par la définition d'un entier pair, $n = 2k$ pour un entier k. En substituant $2k$ à n, on trouve que $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Cela nous dit que $3n + 2$ est pair (car il est un multiple de 2), et donc pas étrange.C'est la négation de la prémisse du théorème. Parce que la négation de la conclusion de l'énoncé conditionnel implique que l'hypothèse est false, l'instruction conditionnelle d'origine est vraie. Notre preuve par contraposition a réussi; nous ont prouvé le théorème "Si $3n + 2$ est impair, alors n est impair." ▲

EXEMPLE 4 Démontrer que si $n = ab$, où a et b sont des entiers positifs, alors $a \le \sqrt{n}$ ou $b \le \sqrt{n}$.

Solution: Parce qu'il n'y a pas de façon évidente de montrer que $a \le \sqrt{n}$ ou $b \le \sqrt{n}$ directement depuis l'équation $n = ab$, où a et b sont des entiers positifs, nous tentons une preuve par contraposition.

La première étape d'une preuve par contraposition est de supposer que la conclusion de la conditionnelle «Si $n = ab$, où a et b sont des entiers positifs, alors $a \le \sqrt{n}$ ou $b \le \sqrt{n}$ "est faux. Cette est, nous supposons que la déclaration $(a \le \sqrt{n}) \vee (b \le \sqrt{n})$ est faux. Utiliser le sens de la disjonction avec la loi de De Morgan, nous voyons que cela implique que les deux $a \le \sqrt{n}$ et $b \le \sqrt{n}$ sont faux. Cela implique qu'un $> \sqrt{n}$ et $b > \sqrt{n}$. On peut multiplier ces inégalités ensemble (en utilisant le fait que si $0 < s < t$ et $0 < u < v$, alors $su < tv$) pour obtenir $ab > \sqrt{n} \cdot \sqrt{n} = n$. Ceci montre que $ab \ne n$, ce qui contredit l'énoncé $n = ab$.

Parce que la négation de la conclusion de l'énoncé conditionnel implique que l'hypothèse esis est faux, l'énoncé conditionnel d'origine est vrai.Notre preuve par contraposition a réussi; nous avons prouvé que si $n = ab$, où a et b sont des entiers positifs, alors $a \le \sqrt{n}$ ou $b \le \sqrt{n}$. ▲

PREUVES VACUES ET TRIVIALES Nous pouvons rapidement prouver qu'une déclaration conditionnelle $p \to q$ est vrai quand on sait que p est faux, car $p \to q$ doit être vrai quand p est faux. Par conséquent, si nous pouvons montrer que p est faux, alors nous avons une preuve, appelée **preuve vide**, de l'instruction conditionnelle $p \to q$. Les preuves vides sont souvent utilisées pour établir des cas particuliers de théorèmes qui indiquent qu'une déclaration conditionnelle est vraie pour tous les entiers positifs [c'est-à-dire un théorème du type $\forall nP(n)$, où $P(n)$ est une fonction propositionnelle]. Techniques de preuve pour les théorèmes de ce type sera discuté dans la section 5.1.

EXEMPLE 5 Montrer que la proposition $P(0)$ est vraie, où $P(n)$ est «Si $n > 1$, alors $n^2 > n$» et le domaine se compose de tous les entiers.

Solution: Notez que $P(0)$ est «Si $0 > 1$, alors $0^2 > 0$». Nous pouvons montrer $P(0)$ *en* utilisant un vide preuve. En effet, l'hypothèse $0 > 1$ est fausse. Cela nous indique que $P(0)$ est automatiquement vrai. ▲

Remarque: Le fait que la conclusion de cette déclaration conditionnelle, $0^2 > 0$, soit fausse n'est pas pertinent à la valeur de vérité de l'instruction conditionnelle, car une instruction conditionnelle avec un faux l'hypothèse est garantie pour être vraie.

On peut aussi rapidement prouver une conditionnelle $p \to q$ si on sait que la conclusion q est vrai. En montrant que q est vrai, il s'ensuit que $p \to q$ doit également être vrai. Une preuve de $p \to q$ qui utilise le fait que q est vrai est appelé une **preuve triviale**. Les preuves triviales sont souvent importantes lorsque des cas particuliers de théorèmes sont prouvés (voir la discussion de la preuve par cas dans la section 1.8) et en induction mathématique, qui est une technique de preuve discutée dans la section 5.1.

EXEMPLE 6 Soit $P(n)$ «Si a et b sont des entiers positifs avec $a \geq b$, alors $a^n \geq b^n$ ", Où le domaine se compose de tous les entiers non négatifs. Montrez que $P(0)$ est vrai.

Solution: La proposition $P(0)$ est «Si $a \geq b$, alors $a^0 \geq b^0$ ». Parce *que* $a^0 = b^0 = 1$, la conclusion de l'énoncé conditionnel «Si $a \geq b$, alors $a^0 \geq b^0$ » est vrai. Par conséquent, cette déclaration conditionnelle, qui est $P(0)$, est vrai. Ceci est un exemple d'une preuve triviale. Notez que l'hypothèse, qui est la mention « $a \geq b$ » n'était pas nécessaire dans cette preuve. ▲

UNE PETITE STRATÉGIE DE PREUVE Nous avons décrit deux approches importantes pour prouver théorèmes de la forme $\forall x (P(x) \to Q(x))$: preuve directe et preuve par contraposition. Nous avons également donné des exemples qui montrent comment chacun est utilisé. Cependant, lorsque vous êtes présenté avec un théorème de la forme $\forall x (P(x) \to Q(x))$, quelle méthode devez-vous utiliser pour tenter de le prouver? Nous fournirons ici quelques règles générales; dans la section 1.8, nous discuterons de la stratégie de preuve longueur. Lorsque vous voulez prouver une déclaration de la forme $\forall x (P(x) \to Q(x))$, évaluez d'abord si une preuve directe semble prometteuse. Commencez par développer les définitions dans les hypothèses. Commencez à raisonner en utilisant ces hypothèses, ainsi que les axiomes et les théorèmes disponibles Si un direct la preuve ne semble aller nulle part, essayez la même chose avec une preuve par contraposition. Rappel que dans une preuve par opposition, vous supposez que la conclusion de la déclaration conditionnelle est false et utiliser une preuve directe pour montrer cela implique que l'hypothèse doit être fausse. Nous illustrons cette stratégie dans les exemples 7 et 8. Avant de présenter notre prochain exemple, nous avons besoin d'une définition.

DÉFINITION 2 Le nombre réel r est *rationnel* s'il existe des entiers p et q avec $q = 0$ tels que $r = p / q$.
Un nombre réel qui n'est pas rationnel est appelé *irrationnel* .

EXEMPLE 7 Montrer que la somme de deux nombres rationnels est rationnelle. (Notez que si nous incluons l'implicite quantificateurs ici, le théorème que nous voulons prouver est «Pour chaque nombre réel r et chaque réel nombre s , si r et s sont des nombres rationnels, alors $r + s$ est rationnel.)

Solution: Nous essayons d'abord une preuve directe. Pour commencer, supposons que r et s sont des nombres rationnels. De la définition d'un nombre rationnel, il s'ensuit qu'il existe des entiers p et q , avec $q = 0$, tels que $r = p / q$, et les entiers t et u , avec $u = 0$, tels que $s = t / u$. Pouvons-nous utiliser ces informations montrer que $r + s$ est rationnel? La prochaine étape évidente consiste à ajouter $r = p / q$ et $s = t / u$, pour obtenir

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu} .$$

Parce que $q = 0$ et $u = 0$, il s'ensuit que $qu = 0$. Par conséquent, nous avons exprimé $r + s$ comme le rapport de deux entiers, $pu + qt$ et qu , où $qu = 0$. Cela signifie que $r + s$ est rationnel. nous ont prouvé que la somme de deux nombres rationnels est rationnelle; notre tentative de trouver une preuve directe réussi. ▲

EXEMPLE 8 Démontrer que si n est un entier et n^2 est impair, alors n est impair.

Solution: Nous essayons d'abord une preuve directe. Supposons que n est un entier et n^2 est impair. Ensuite, là existe un entier k tel que $n^2 = 2k + 1$. Pouvons-nous utiliser cette information pour montrer que n est impair? Il ne semble pas y avoir d'approche évidente pour montrer que n est impair car la résolution de n produit l'équation $n = \pm \sqrt{2k + 1}$, ce qui n'est pas terriblement utile.

Parce que cette tentative d'utilisation d'une preuve directe n'a pas porté ses fruits, nous tentons ensuite une preuve par contraposition. Nous prenons comme hypothèse l'affirmation que n n'est pas impair. Parce que chaque entier est impair ou pair, cela signifie que n est pair. Cela implique qu'il existe un entier k tel que $n = 2k$. Pour prouver le théorème, nous devons montrer que cette hypothèse implique la conclusion que n^2 n'est pas impair, c'est-à-dire que n^2 est pair. Pouvons-nous utiliser l'équation $n = 2k$ pour y parvenir? Par

au carré des deux côtés de cette équation, on obtient $n^2 = 4k^2 = 2(2k^2)$, ce qui implique que n^2 est même parce que $n^2 = 2t$, où $t = 2k^2$. Nous avons prouvé que si n est un entier et n^2 est impair, ▲

alors n est impair. Notre tentative de trouver une preuve par contraposition a réussi.

Preuves par contradiction

Supposons que nous voulons prouver qu'une déclaration p est vraie. De plus, supposons que l'on puisse trouver une contradiction q telle que $\neg p \rightarrow q$ est vraie. Parce que q est faux, mais $\neg p \rightarrow q$ est vrai, nous pouvons conclure que $\neg p$ est faux, ce qui signifie que p est vrai. Comment pouvons - nous trouver une contradiction q que pourrait nous aider à prouver que p est vrai de cette façon?

Parce que l'énoncé $r \wedge \neg r$ est une contradiction chaque fois que r est une proposition, nous pouvons prouver que p est vrai si nous pouvons montrer que $\neg p \rightarrow (r \wedge \neg r)$ est vrai pour une proposition r. Des preuves de cela type sont appelés **preuves par contradiction**. Parce qu'une preuve par contradiction ne prouve pas un résultat directement, c'est un autre type de preuve indirecte. Nous fournissons trois exemples de preuve par contradiction. Le premier est un exemple d'application du principe du pigeonhole, une technique combinatoire que nous aborderons en détail dans la section 6.2.

EXEMPLE 9 Montrez qu'au moins quatre des 22 jours doivent tomber le même jour de la semaine.

Solution: Soit p la proposition «Au moins quatre des 22 jours choisis tombent le même jour de la semaine. »Supposons que $\neg p$ est vrai. Cela signifie qu'au plus trois des 22 jours tombent sur le même jour de la semaine. Parce qu'il y a sept jours de la semaine, cela implique qu'au plus 21 jours aurait pu être choisi, comme pour chacun des jours de la semaine, au plus trois des jours choisis pourrait tomber ce jour-là. Cela contredit l'hypothèse selon laquelle nous avons 22 jours à l'étude. Autrement dit, si r est la déclaration que 22 jours sont choisis, alors nous avons montré que $\neg p \rightarrow (r \wedge \neg r)$. Par conséquent, nous savons que p est vrai. Nous avons prouvé qu'au moins quatre des 22 jours choisis tombent le même jour de la semaine. ▲

EXEMPLE 10 Prouver que $\sqrt{2}$ est irrationnel en donnant une preuve par contradiction.

Solution: Soit p la proposition " $\sqrt{2}$ est irrationnel. »Pour commencer une preuve par contradiction, nous supposons que $\neg p$ est vrai. Notez que $\neg p$ est la déclaration «Ce n'est pas le cas que $\sqrt{2}$ est irrationnel », ce qui dit ça $\sqrt{2}$ est rationnel. Nous montrerons que supposer que $\neg p$ est vrai conduit à une contradiction.

Si $\sqrt{2}$ est rationnel, il existe des entiers a et b avec $\sqrt{2} = a / b$, où $b \neq 0$ et a et b n'ont pas de facteurs communs (de sorte que la fraction a / b est en termes les plus bas.) (Ici, nous utilisons le fait que chaque nombre rationnel peut être écrit en termes les plus bas.) Parce que $\sqrt{2} = a / b$, lorsque les deux côtés de cette équation sont au carré, il s'ensuit que

$$2 = \frac{a^2}{b^2}.$$

Par conséquent,

$$2b^2 = a^2.$$

Par la définition d'un nombre entier, même il en résulte que a^2 est même. Nous utilisons ensuite le fait que si a^2 est même, a doit aussi être pair, ce qui suit par l'exercice 16. De plus, parce que a est pair, par la définition d'un entier pair, $a = 2c$ pour un entier c. Donc,

$$2b^2 = 4c^2.$$

La division des deux côtés de cette équation par 2 donne

$$b^2 = 2c^2.$$

Par la définition de pair, cela signifie que b^2 est pair. En utilisant à nouveau le fait que si le carré d'un entier est pair, alors l'entier lui-même doit être pair, nous concluons que b doit aussi être pair.

Nous avons maintenant montré que l'hypothèse de $\neg p$ conduit à l'équation $\sqrt{2} = a / b$, où a et b n'ont pas de facteurs communs, mais a et b sont pairs, c'est-à-dire que 2 divise à la fois a et b. Remarque que la déclaration $\sqrt{2} = a / b$, où a et b n'ont pas de facteurs communs, signifie, en particulier, que 2 ne divise pas à la fois a et b. Parce que notre hypothèse de $\neg p$ conduit à la contradiction que 2 divise à la fois a et b et 2 ne divise pas à la fois a et b, $\neg p$ doit être faux. C'est le déclaration p, " $\sqrt{2}$ est irrationnel », est vrai. Nous avons prouvé que $\sqrt{2}$ est irrationnel. ▲

La preuve par contradiction peut être utilisée pour prouver des déclarations conditionnelles. Dans de telles preuves, nous assumer la négation de la conclusion. Nous utilisons ensuite les prémisses du théorème et de la négation de la conclusion pour arriver à une contradiction. (La raison pour laquelle ces preuves sont valables repose sur équivalence logique de $p \rightarrow q$ et $(p \wedge \neg q) \rightarrow \mathbf{F}$. Pour voir que ces déclarations sont équivalentes, notez simplement que chacun est faux dans exactement un cas, à savoir lorsque p est vrai et q est faux.)

Notez que nous pouvons réécrire une preuve en contraposant un énoncé conditionnel comme preuve par contradiction. Dans une preuve de $p \rightarrow q$ par contraposition, nous supposons que $\neg q$ est vrai. Nous avons ensuite montrer que $\neg p$ doit également être vrai. Réécrire une preuve par contraposition de $p \rightarrow q$ comme preuve par contradiction, nous supposons que p et $\neg q$ sont vrais. Ensuite, nous utilisons les étapes de la preuve de $\neg q \rightarrow \neg p$ pour montrer que $\neg p$ est vrai. Cela conduit à la contradiction $p \wedge \neg p$, complétant la preuve. L'exemple 11 illustre comment une preuve par contraposition d'une déclaration conditionnelle peut être réécrit comme preuve par contradiction.

EXEMPLE 11 Donner une preuve par contradiction du théorème "Si $3n + 2$ est impair, alors n est impair."

Solution: Soit p «$3n + 2$ est impair» et q soit « n est impair». Pour construire une preuve par contradiction, supposons que p et $\neg q$ sont vrais. Autrement dit, supposons que $3n + 2$ est impair et que n n'est pas impair. Parce que n n'est pas impair, nous savons qu'il est pair. Parce que n est pair, il existe un entier k tel que $n = 2k$. Cela implique que $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Parce que $3n + 2$ est $2t$, où $t = 3k + 1$, $3n + 2$ est pair. Notez que l'énoncé «$3n + 2$ est pair» équivaut à l'énoncé $\neg p$, car un entier est pair si et seulement s'il n'est pas impair. Parce que p et $\neg p$ sont vrais, nous avons une contradiction. Ceci complète la preuve par contradiction, prouvant que si $3n + 2$ est impair, alors n est impair. ▲

Notez que nous pouvons également prouver par contradiction que $p \rightarrow q$ est vrai en supposant que p et $\neg q$ sont vrais, et montrant que q doit également être vrai. Cela implique que $\neg q$ et q sont tous les deux vrai, une contradiction. Cette observation nous dit que nous pouvons transformer une preuve directe en une preuve en contradiction.

PREUVES D'ÉQUIVALENCE Pour prouver un théorème qui est un énoncé biconditionnel, c'est-à-dire: un énoncé de la forme $p \leftrightarrow q$, nous montrons que $p \rightarrow q$ et $q \rightarrow p$ sont tous deux vrais. La validité de cette approche est basée sur la tautologie

$$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p).$$

EXEMPLE 12 Démontrer le théorème "Si n est un entier, alors n est impair si et seulement si n^2 est impair."

Solution: ce théorème a la forme «p si et seulement si q », où p est « n est impair» et q est « n^2 est étrange. »(Comme d'habitude, nous ne traitons pas explicitement de la quantification universelle.) Pour le prouver théorème, nous devons montrer que $p \rightarrow q$ et $q \rightarrow p$ sont vrais.

Nous avons déjà montré (dans l'exemple 1) que $p \rightarrow q$ est vrai et (dans l'exemple 8) que $q \rightarrow p$ est vrai.

Parce que nous avons montré que $p \rightarrow q$ et $q \rightarrow p$ sont vrais, nous avons montré que le le théorème est vrai. ▲

Parfois, un théorème déclare que plusieurs propositions sont équivalentes. Un tel théorème déclare que les propositions $p_1, p_2, p_3, \ldots, p_n$ sont équivalentes. Cela peut être écrit comme

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n,$$

qui déclare que toutes les n propositions ont les mêmes valeurs de vérité, et par conséquent, que pour tout i et j avec $1 \leq i \leq n$ et $1 \leq j \leq n$, p_i et p_j sont équivalents. Une façon de le prouver mutuellement l'équivalent est d'utiliser la tautologie

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \leftrightarrow (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \cdots \wedge (p_n \rightarrow p_1).$$

Cela montre que si les n instructions conditionnelles $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, ..., $p_n \rightarrow p_1$ peuvent être affichées pour être vrai, alors les propositions $p_1, p_2, \ldots, p_n$ sont toutes équivalentes.

Ceci est beaucoup plus efficace que de prouver que $p_i \rightarrow p_j$ pour tout $i = j$ avec $1 \leq i \leq n$ et $1 \leq j \leq n$. (Notez qu'il existe $n^2 - n$ de telles instructions conditionnelles.)

Lorsque nous prouvons qu'un groupe de déclarations est équivalent, nous pouvons établir une chaîne de déclarations conditionnelles que nous choisissons aussi longtemps qu'il est possible de travailler à travers la chaîne pour aller de n'importe laquelle de ces déclarations à toute autre déclaration. Par exemple, nous pouvons montrer que p_1, p_2 et p_3 sont équivalents en montrant que $p_1 \rightarrow p_3$, $p_3 \rightarrow p_2$ et $p_2 \rightarrow p_1$.

EXEMPLE 13 Montrez que ces déclarations sur l'entier n sont équivalentes:

p_1 : n est pair.
p_2 : $n - 1$ est impair.
p_3 : n^2 est pair.

Solution: Nous montrerons que ces trois déclarations sont équivalentes en montrant que le conditionnel les énoncés $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$ et $p_3 \rightarrow p_1$ sont vrais.

Nous utilisons une preuve directe pour montrer que $p_1 \rightarrow p_2$. Supposons que n soit pair. Alors $n = 2k$ pour certains entier k. Par conséquent, $n - 1 = 2k - 1 = 2(k - 1) + 1$. Cela signifie que $n - 1$ est impair car il est de la forme $2m + 1$, où m est l'entier $k - 1$.

Nous utilisons également une preuve directe pour montrer que $p_2 \rightarrow p_3$. Supposons maintenant que $n - 1$ soit impair. Alors $n - 1 = 2k + 1$ pour un entier k. Par conséquent, $n = 2k + 2$ de sorte que $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$. Cela signifie que n^2 est le double de l'entier $2k^2 + 4k + 2$, et est donc pair.

Pour prouver $p_3 \rightarrow p_1$, nous utilisons une preuve par contraposition. Autrement dit, nous prouvons que si n n'est pas pair, alors n^2 n'est pas pair. Cela revient à prouver que si n est impair, alors n^2 est impair, ce que nous avons déjà fait dans l'exemple 1. Ceci complète la preuve. ▲

CONTRE-EXEMPLES Dans la section 1.4, nous avons déclaré que pour montrer qu'une déclaration du formulaire $\forall x P(x)$ est faux, il suffit de trouver un **contre - exemple**, c'est-à-dire un exemple x pour lequel $P(x)$ c'est faux. Lorsqu'on lui présente une déclaration de la forme $\forall x P(x)$, que nous croyons être fausse ou qui a résisté à toutes les tentatives de preuve, nous recherchons un contre-exemple. Nous illustrons l'utilisation de contre-exemples dans l'exemple 14.

EXEMPLE 14 Montrer que l'énoncé «Chaque entier positif est la somme des carrés de deux entiers» est faux.

Solution: pour montrer que cette affirmation est fausse, nous recherchons un contre-exemple, qui est un entier qui n'est pas la somme des carrés de deux entiers. Il ne faut pas longtemps pour trouver une contre-ample, car 3 ne peut pas être écrit comme la somme des carrés de deux entiers Pour montrer que c'est Dans ce cas, notez que les seuls carrés parfaits ne dépassant pas 3 sont $0^2 = 0$ et $1^2 = 1$. De plus, il n'y a aucun moyen d'obtenir 3 comme la somme de deux termes dont chacun est 0 ou 1. Par conséquent, nous avons a montré que "Chaque entier positif est la somme des carrés de deux entiers" est faux. ▲

Erreurs dans les épreuves

Il existe de nombreuses erreurs courantes dans la construction de preuves mathématiques. Nous allons brièvement décrire certains d'entre eux ici. Parmi les erreurs les plus courantes figurent les erreurs d'arithmétique et de base algèbre. Même les mathématiciens professionnels font de telles erreurs, surtout lorsqu'ils travaillent avec formules compliquées. Chaque fois que vous utilisez de tels calculs, vous devez les vérifier avec autant de soin que possible. (Vous devez également passer en revue tous les aspects gênants de l'algèbre de base, en particulier avant vous étudiez la section 5.1.)

Chaque étape d'une preuve mathématique doit être correcte et la conclusion doit suivre logiquement des étapes qui la précèdent. De nombreuses erreurs résultent de l'introduction d'étapes qui ne découlent pas logiquement de ceux qui le précèdent. Ceci est illustré dans les exemples 15 à 17.

EXEMPLE 15 Quel est le problème avec cette fameuse "preuve" supposée que 1 = 2?

"Preuve:" Nous utilisons ces étapes, où a et b sont deux entiers positifs égaux.

Étape	**Raison**
1. $a = b$	Donné
2. $a^2 = ab$	Multipliez les deux côtés de (1) par *un*
3. $a^2 - b^2 = ab - b^2$	Soustrayez b^2 des deux côtés de (2)
4. $(a - b)(a + b) = b(a - b)$	Factoriser les deux côtés de (3)
5. $a + b = b$	Divisez les deux côtés de (4) par $a - b$
6. $2b = b$	Remplacez a par b dans (5) car $a = b$ et simplifier
7. $2 = 1$	Divisez les deux côtés de (6) par b

Solution: Chaque étape est valide sauf une, étape 5 où nous avons divisé les deux côtés par $a - b$. le l'erreur est que $a - b$ est égal à zéro; la division des deux côtés d'une équation par la même quantité est valable tant que cette quantité n'est pas nulle. ▲

EXEMPLE 16 Quel est le problème avec cette «preuve»?

«Théorème:» Si n^2 est positif, alors n est positif.

"Preuve:" Supposons que n^2 soit positif. Parce que l'énoncé conditionnel "Si n est positif, alors n^2 est positif »est vrai, nous pouvons conclure que n est positif.

Solution: Soit $P(n)$ soit « n est positif» et $Q(n)$ soit « n^2 est positif». Alors notre hypothèse est $Q(n)$. L'énoncé «Si n est positif, alors n^2 est positif» est l'énoncé $\forall n (P(n) \rightarrow Q(n))$. De l'hypothèse $Q(n)$ et l'énoncé $\forall n (P(n) \rightarrow Q(n))$ nous ne pouvons pas conclure $P(n)$, car nous n'utilisons pas de règle d'inférence valide. Au lieu de cela, ceci est un exemple de l'erreur d'affirmer la conclusion. Un contre-exemple est fourni par $n = -1$ pour lequel $n^2 = 1$ est positif, mais n est négatif. ▲

EXEMPLE 17 Quel est le problème avec cette «preuve»?

"Théorème:" Si n n'est pas positif, alors n^2 n'est pas positif. (C'est la contrapositive de la «Théorème» dans l'exemple 16.)

"Preuve:" Supposons que n n'est pas positif. Parce que l'énoncé conditionnel "Si n est positif, alors n^2 est positif »est vrai, nous pouvons conclure que n^2 n'est pas positif.

Solution: Soit $P(n)$ et $Q(n)$ comme dans la solution de l'exemple 16. Alors notre hypothèse est $\neg P(n)$ et la déclaration «Si n est positif, alors n^2 est positif» est la déclaration $\forall n\,(P(n) \rightarrow Q(n))$. A partir de l'hypothèse $\neg P(n)$ et de l'énoncé $\forall n\,(P(n) \rightarrow Q(n))$ nous ne pouvons pas conclure $\neg Q(n)$, parce que nous n'utilisons pas de règle d'inférence valide. Au lieu de cela, ceci est un exemple de l'erreur de niant l'hypothèse. Un contre-exemple est fourni par $n = -1$, comme dans l'exemple 16. ▲

Enfin, nous discutons brièvement d'un type d'erreur particulièrement désagréable. De nombreux arguments incorrects sont basé sur une erreur appelée **mendier la question** . Cette erreur se produit lorsqu'une ou plusieurs étapes de une preuve est basée sur la véracité de la déclaration en cours de preuve. En d'autres termes, cette erreur se pose lorsqu'une instruction est prouvée en utilisant elle-même, ou une instruction équivalente à celle-ci. Voilà pourquoi cette erreur est aussi appelé **raisonnement circulaire** .

EXEMPLE 18 L'argument suivant est-il correct? Il montre que n est un entier pair chaque fois que n^2 est un entier pair.

Supposons que n^2 soit pair. Alors $n^2 = 2k$ pour un entier k . Soit $n = 2l$ pour un entier l . Cela montre que n est pair.

Solution: cet argument est incorrect. L'instruction «soit $n = 2l$ pour un entier l » apparaît dans la preuve. Aucun argument n'a été donné pour montrer que n peut être écrit comme $2l$ pour un entier l . Ceci est un raisonnement circulaire car cette déclaration est équivalente à la déclaration étant prouvée, à savoir, « n est pair». Bien sûr, le résultat lui-même est correct; seule la méthode de preuve est fausse. ▲

Faire des erreurs dans les épreuves fait partie du processus d'apprentissage. Lorsque vous faites une erreur quelqu'un d'autre trouve, vous devez soigneusement analyser où vous vous êtes trompé et vous assurer que vous ne faites plus la même erreur. Même les mathématiciens professionnels font des erreurs preuves. Plus de quelques preuves incorrectes de résultats importants ont trompé les gens pendant de nombreuses années avant que de subtiles erreurs ne soient trouvées.

Juste un début

Nous avons maintenant développé un arsenal de base de méthodes de preuve. Dans la section suivante, nous présenterons d'autres méthodes de preuve importantes. Nous présenterons également plusieurs techniques de preuve importantes dans Le chapitre 5, y compris l'induction mathématique, qui peut être utilisé pour prouver des résultats qui tous les entiers positifs. Dans le chapitre 6, nous introduirons la notion de preuves combinatoires.

Dans cette section, nous avons introduit plusieurs méthodes pour prouver les théorèmes de la forme $\forall x\,(P(x) \rightarrow Q(x))$, y compris les preuves directes et les preuves par contraposition. Il existe de nombreux théorèmes de cette type dont les preuves sont faciles à construire en travaillant directement à travers les hypothèses et initions des termes du théorème. Cependant, il est souvent difficile de prouver un théorème sans recourir à une utilisation intelligente d'une preuve par contraposition ou d'une preuve par contradiction, ou autre technique de preuve. Dans la section 1.8, nous aborderons la stratégie de preuve. Nous décrirons divers approches qui peuvent être utilisées pour trouver des preuves lorsque les approches simples ne fonctionnent pas. Con-La structuration des preuves est un art qui ne s'apprend que par l'expérience, y compris la rédaction de preuves, faire critiquer vos épreuves et lire et analyser d'autres épreuves.

Des exercices

1. Utilisez une preuve directe pour montrer que la somme de deux entiers impairs est même.

2. Utilisez une preuve directe pour montrer que la somme de deux entiers pairs gers est encore.

3. Montrez que le carré d'un nombre pair est un nombre pair en utilisant une preuve directe.

4. Montrer que l'inverse additif, ou négatif, d'un pair nombre est un nombre pair utilisant une preuve directe.

5. Montrer que si $m + n$ et $n + p$ sont des entiers pairs, où m, n et p sont des entiers, alors $m + p$ est pair. Quel genre de preuve avez-vous utilisé?

6. Utilisez une preuve directe pour montrer que le produit de deux les nombres sont impairs.

7. Utilisez une preuve directe pour montrer que chaque entier impair est le différence de deux carrés.

8. Montrer que si n est un carré parfait, alors $n + 2$ n'est pas un un carré parfait.

9. Utiliser une preuve par contradiction pour prouver que la somme d'un nombre irrationnel et un nombre rationnel est irrationnel.

10. Utilisez une preuve directe pour montrer que le produit de deux les chiffres sont rationnels.

11. Prouver ou infirmer que le produit de deux nombres irrationnels bers est irrationnel.

12. Prouver ou infirmer que le produit d'un rationnel non nul nombre et un nombre irrationnel est irrationnel.

13. Démontrez que si x est irrationnel, alors $1/x$ est irrationnel.

14. Montrer que si x est rationnel et $x = 0$, alors $1/x$ est rationnel.

15. Utilisez une preuve par contraposition pour montrer que si $x + y \geq 2$, où x et y sont des nombres réels, alors $x \geq 1$ ou $y \geq 1$.

16. Démontrer que si m et n sont des entiers et mn est pair, alors m est pair ou n est pair.

17. Montrer que si n est un entier et $n^3 + 5$ est impair, alors n est même en utilisant

a) une preuve par contraposition.

b) une preuve par contradiction.

18. Montrer que si n est un entier et $3n + 2$ est pair, alors n est même en utilisant

a) une preuve par contraposition.

b) une preuve par contradiction.

19. Démontrer la proposition $P(0)$, où $P(n)$ est la proposition «Si n est un entier positif supérieur à 1, alors $n^2 > n$.» Quel type de preuve avez-vous utilisé?

20. Démontrer la proposition $P(1)$, où $P(n)$ est la proposition «Si n est un entier positif, alors $n^2 \geq n$.» Quel type de preuve avez-vous utilisé?

21. Soit $P(n)$ la proposition «Si a et b sont réels réels nombres, alors $(a + b)^n \geq a^n + b^n$.» Montrer que $P(1)$ est vrai. Quel type de preuve avez-vous utilisé?

22. Montrez que si vous choisissez trois chaussettes dans un tiroir contenant avec des chaussettes bleues et des chaussettes noires, vous devez une paire de chaussettes bleues ou une paire de chaussettes noires.

23. Montrez qu'au moins dix des 64 jours choisis doivent tomber sur le même jour de la semaine.

24. Montrez qu'au moins trois des 25 jours choisis doivent tomber au cours du même mois de l'année.

25. Utilisez une preuve par contradiction pour montrer qu'il n'existe pas de nombre final r pour lequel $r^3 + r + 1 = 0$. [*Indice:* Supposons que $r = a/b$ est une racine, où a et b sont des entiers et a/b est en termes les plus bas. Obtenir une équation impliquant des entiers en multipliant par b^3. Regardez ensuite si a et b sont chacun impair ou pair.]

26. Démontrer que si n est un entier positif, alors n est pair si et seulement si $7n + 4$ est pair.

27. Démontrer que si n est un entier positif, alors n est impair si et seulement si $5n + 6$ est impair.

28. Montrer que $m^2 = n^2$ si et seulement si $m = n$ ou $m = -n$.

29. Prouver ou infirmer que si m et n sont des entiers tels que $mn = 1$, alors soit $m = 1$ et $n = 1$, soit $m = -1$ et $n = -1$.

30. Montrer que ces trois déclarations sont équivalentes, où *un* et b sont des nombres réels: (*i*) a est inférieur à b, (*ii*) la moyenne de a et b est supérieur à a, et (*iii*) la moyenne de a et b est inférieur à b.

31. Montrer que ces déclarations sur l'entier x sont équivalentes alentour: (*i*) $3x + 2$ est pair, (*ii*) $x + 5$ est impair, (*iii*) x^2 est pair.

32. Montrer que ces déclarations sur le nombre réel x sont équivalent: (*i*) x est rationnel, (*ii*) $x/2$ est rationnel, (*iii*) $3x - 1$ est rationnel.

33. Montrer que ces déclarations sur le nombre réel x sont équivalent: (*i*) x est irrationnel, (*ii*) $3x + 2$ est irrationnel, (*iii*) $x/2$ est irrationnel.

34. Est-ce ce raisonnement pour trouver les solutions de l'équation $\sqrt{2x^2 - 1} = x$ correct? (*1*) $\sqrt{2x^2 - 1} = x$ est donné; (*2*) $2x^2 - 1 = x^2$, obtenu en quadrillant les deux côtés de (1); (*3*) $x^2 - 1 = 0$, obtenu en soustrayant x^2 des deux côtés de (2); (*4*) $(x - 1)(x + 1) = 0$, obtenu par facteur- sur le côté gauche de $x^2 - 1$; (*5*) $x = 1$ ou $x = -1$, qui suit parce que $ab = 0$ implique que $a = 0$ ou $b = 0$.

35. Ces étapes sont-elles nécessaires pour trouver les solutions $\sqrt{x + 3} = 3 - x$ correct? *(1)* $\sqrt{x + 3} = 3 - x$ est donné; (*2*) $x + 3 = x^2 - 6x + 9$, obtenu en mettant au carré les deux côtés de (1) ; (*3*) $0 = x^2 - 7x + 6$, obtenu en soustrayant $x + 3$ de les deux côtés de (2) ; (*4*) $0 = (x - 1)(x - 6)$, obtenu par factoriser le côté droit de (3) ; (*5*) $x = 1$ ou $x = 6$, qui découle de (4) car $ab = 0$ implique que $a = 0$ ou $b = 0$.

36. Montrer que les propositions p_1, p_2, p_3 et p_4 peuvent être montré comme équivalent en montrant que $p_1 \leftrightarrow p_4$, $p_2 \leftrightarrow p_3$ et $p_1 \leftrightarrow p_3$.

37. Montrer que les propositions p_1, p_2, p_3, p_4 et p_5 peuvent être équivalente en prouvant que la conditionnelle déclarations $p_1 \rightarrow p_4$, $p_3 \rightarrow p_1$, $p_4 \rightarrow p_2$, $p_2 \rightarrow p_5$, et $p_5 \rightarrow p_3$ sont vrais.

38. Trouvez un contre-exemple de l'affirmation selon laquelle chaque posi- entier positif peut être écrit comme la somme des carrés de trois entiers.

39. Démontrer qu'au moins un des nombres réels $a_1, a_2, \ldots, a_n$ est supérieur ou égal à la moyenne de ces nombres. Quel type de preuve avez-vous utilisé?

40. Utilisez l'exercice 39 pour montrer que si les 10 premiers Les gers sont placés autour d'un cercle, dans n'importe quel ordre, il existe trois entiers dans des emplacements consécutifs autour du cercle dont la somme est supérieure ou égale à 17.

41. Montrer que si n est un entier, ces quatre déclarations sont équivalent: (i) n est pair, (ii) $n + 1$ est impair, (iii) $3n + 1$ est impair, (iv) $3n$ est pair.

42. Montrer que ces quatre déclarations sur l'entier n sont équivalent: (i) n^2 est impair, (ii) $1 - n$ est pair, (iii) n^3 est impair, (iv) $n^2 + 1$ est pair.

Méthodes et stratégie de preuve

introduction

Dans la section 1.7, nous avons présenté de nombreuses méthodes de preuve et illustré comment chaque méthode peut être utilisé. Dans cette section, nous poursuivons cet effort. Nous présenterons plusieurs autres preuves couramment utilisées méthodes, y compris la méthode de démonstration d'un théorème en considérant différents cas séparément. Nous discuterons également des preuves où nous prouvons l'existence d'objets ayant les propriétés souhaitées.

Dans la section 1.7, nous avons brièvement discuté de la stratégie derrière la construction de preuves.Cette stratégie comprend la sélection d'une méthode de preuve puis la construction réussie d'un argument étape par étape, basé sur cette méthode. Dans cette section, après avoir développé un arsenal de preuve polyvalent méthodes, nous étudierons certains aspects de l'art et de la science des preuves.Nous vous conseillerons sur la façon de trouver une preuve d'un théorème. Nous décrirons quelques astuces du métier, y compris comment les preuves peuvent être trouvées en travaillant à l'envers et en adaptant les preuves existantes.

Lorsque les mathématiciens travaillent, ils formulent des conjectures et tentent de prouver ou de réfuter leur. Nous allons décrire brièvement ce processus ici en prouvant les résultats sur les carreaux en damier avec dominos et autres types de pièces. En regardant des pavages de ce type, nous pourrons formuler rapidement des conjectures et prouver des théorèmes sans d'abord développer une théorie.

Nous terminerons la section en discutant du rôle des questions ouvertes.En particulier, nous discutera de quelques problèmes intéressants qui ont été résolus après être restés ouverts pendant des centaines d'années ou qui restent encore ouvertes.

Preuve exhaustive et preuve par cas

Parfois, nous ne pouvons pas prouver un théorème en utilisant un seul argument valable pour tous les cas possibles. Nous introduisons maintenant une méthode qui peut être utilisée pour prouver un théorème, en considérant différents cas séparément. Cette méthode est basée sur une règle d'inférence que nous allons maintenant introduire. Pour prouver un déclaration conditionnelle du formulaire

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$$

la tautologie

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)]$$

peut être utilisé comme règle d'inférence.Cela montre que l'instruction conditionnelle d'origine avec une hypothèse constituée d'une disjonction des propositions $p_1, p_2, \ldots, p_n$ peut être démontrée par prouver chacune des n instructions conditionnelles $p_i \to q$, $i = 1, 2, \ldots, n$, individuellement. Un tel L'argument est appelé une **preuve par cas** . Parfois, pour prouver qu'une déclaration conditionnelle $p \to q$ est vrai, il est commode d'utiliser une disjonction $p_1 \vee p_2 \vee \cdots \vee p_n$ au lieu de p comme hypothèse de l'instruction conditionnelle, où p et $p_1 \vee p_2 \vee \cdots \vee p_n$ sont équivalents.

PREUVE EXHAUSTIVE Certains théorèmes peuvent être prouvés en examinant un nombre relativement petit d'exemples. Ces preuves sont appelées **preuves exhaustives** , ou **preuves par épuisement** parce que ces **preuves** les preuves procèdent en épuisant toutes les possibilités.Une preuve exhaustive est un type spécial de preuve par cas où chaque cas implique la vérification d'un seul exemple. Nous fournissons maintenant quelques illustrations de preuves exhaustives.

EXEMPLE 1 Démontrer que $(n+1)^3 \geq 3^n$ si n est un entier positif avec $n \leq 4$.

Solution: Nous utilisons une preuve d'épuisement. Il suffit de vérifier l'inégalité $(n+1)^3 \geq 3^n$ lorsque $n = 1, 2, 3$, et 4. Pour $n = 1$, on a $(n+1)^3 = 2^3 = 8$ et $3^n = 3^1 = 3$; pour $n = 2$, nous avons $(n+1)^3 = 3^3 = 27$ et $3^n = 3^2 = 9$; pour $n = 3$, on a $(n+1)^3 = 4^3 = 64$ et $3^n = 3^3 = 27$; et pour $n = 4$, nous avons $(n+1)^3 = 5^3 = 125$ et $3^n = 3^4 = 81$. Dans chacun de ces quatre cas, on voit que $(n+1)^3 \geq 3^n$. Nous avons utilisé la méthode de l'épuisement pour prouver que $(n+1)^3 \geq 3^n$ si n est un entier positif avec $n \leq 4$. ▲

EXEMPLE 2 Démontrer que les seuls entiers positifs consécutifs ne dépassant pas 100 qui sont des puissances parfaites sont 8 et 9. (Un entier est une **puissance parfaite** s'il est égal à n^a, où a est un entier supérieur à 1.)

Solution: Nous utilisons une preuve d'épuisement. En particulier, nous pouvons prouver ce fait en examinant des entiers positifs n ne dépassant pas 100, en vérifiant d'abord si n est une puissance parfaite, et si elle l'est, vérifier si $n + 1$ est également une puissance parfaite. Un moyen plus rapide de le faire est simplement de regarder puissances parfaites ne dépassant pas 100 et vérifier si le prochain plus grand entier est également parfait Puissance. Les carrés des nombres entiers positifs ne dépassant pas 100 sont 1, 4, 9, 16, 25, 36, 49, 64, 81 et 100. Les cubes d'entiers positifs ne dépassant pas 100 sont 1, 8, 27 et 64. Les quatrièmes puissances des entiers positifs ne dépassant pas 100 sont 1, 16 et 81. Les cinquièmes puissances des entiers positifs ne dépassant pas 100 sont 1 et 32. Les sixièmes puissances d'entiers positifs ne dépassant pas 100 sont 1 et 64. Il n'y a pas de puissances d'entiers positifs supérieurs à la sixième puissance n'excédant pas 100, autre que 1. En regardant cette liste de puissances parfaites ne dépassant pas 100, nous voyons que $n = 8$ est le seule puissance parfaite n pour laquelle $n + 1$ est également une puissance parfaite. Autrement dit, $2^3 = 8$ et $3^2 = 9$ sont les seulement deux puissances parfaites consécutives ne dépassant pas 100. ▲

Les preuves par épuisement peuvent fatiguer les gens et ordinateurs lorsque le Nombre de cas défie le disponible puissance de calcul!

Les gens peuvent effectuer des preuves exhaustives quand il est nécessaire de vérifier seulement un relativement petit nombre d'instances d'une instruction. Les ordinateurs ne se plaignent pas quand on leur demande de vérifier un nombre beaucoup plus élevé d'instances d'une instruction, mais elles ont encore des limites. Notez que non même un ordinateur peut vérifier toutes les instances lorsqu'il est impossible de répertorier toutes les instances à vérifier.

PREUVE PAR CAS Une preuve par cas doit couvrir tous les cas possibles qui surviennent dans un théorème. Nous illustrons la preuve par des cas avec quelques exemples. Dans chaque exemple, vous devez vérifier que tous les cas possibles sont couverts.

EXEMPLE 3 Démontrer que si n est un entier, alors $n^2 \geq n$.

Solution: Nous pouvons prouver que $n^2 \geq n$ pour chaque entier en considérant trois cas, lorsque $n = 0$, quand $n \geq 1$, et quand $n \leq -1$. Nous avons divisé la preuve en trois cas car elle est simple pour prouver le résultat en considérant le zéro, les entiers positifs et les entiers négatifs séparément.

Cas (i): Lorsque $n = 0$, parce que $0^2 = 0$, nous voyons que $0^2 \geq 0$. Il s'ensuit que $n^2 \geq n$ est vrai dans ce cas.

Cas (ii): Quand $n \geq 1$, quand on multiplie les deux côtés de l'inégalité $n \geq 1$ par le positif entier n, on obtient $n \cdot n \geq n \cdot 1$. Cela implique que $n^2 \geq n$ pour $n \geq 1$.

Cas (iii): Dans ce cas $n \leq -1$. Cependant, $n^2 \geq 0$. Il s'ensuit que $n^2 \geq n$.

Parce que l'inégalité $n^2 \geq n$ est vraie dans les trois cas, nous pouvons conclure que si n est un entier, alors $n^2 \geq n$. ▲

EXEMPLE 4 Utilisez une preuve par cas pour montrer que $|xy| = |x||y|$, où x et y sont des nombres réels. (Rappeler que

$|a|$, la valeur absolue de a, est égale à a lorsque $a \geq 0$ et égale $-a$ lorsque $a \leq 0$.)

Solution: Dans notre preuve de ce théorème, nous supprimons les valeurs absolues en utilisant le fait que $|a| = a$ quand $un \geq 0$ et $|a| = -a$ lorsque $a < 0$. Parce que les deux $|x|$ et $|y|$ se produire dans notre formule, nous allons besoin de quatre cas: *(i)* x et y tous deux non négatifs, *(ii)* x non négatifs et y est négatif, *(iii)* x négatifs et y non négatif, et *(iv)* x négatif et y négatif. On note p_1, p_2, p_3 et p_4, le proposition énonçant l'hypothèse pour chacun de ces quatre cas, respectivement.

(Notez que nous pouvons supprimer les signes de valeur absolue en faisant le choix approprié de signes dans chaque cas.)

Cas (i): On voit que $p_1 \to q$ car $xy \geq 0$ quand $x \geq 0$ et $y \geq 0$, de sorte que $|xy| = xy = |x||y|$.

Cas (ii): Pour voir que $p_2 \to q$, notons que si $x \geq 0$ et $y < 0$, alors $xy \leq 0$, de sorte que $|xy| = -xy = x(-y) = |x||y|$. (Ici, parce que $y < 0$, nous avons $|y| = -y$.)

Cas (iii): Pour voir que $p_3 \to q$, nous suivons le même raisonnement que le cas précédent avec le rôles de x et y inversés.

Cas (iv): Pour voir que $p_4 \to q$, notons que lorsque $x < 0$ et $y < 0$, il s'ensuit que $xy > 0$. Par conséquent, $|xy| = xy = (-x)(-y) = |x||y|$.

Parce que $|xy| = |x||y|$ détient dans chacun des quatre cas et ces cas épuisent toutes les possibilités, nous pouvons conclure que $|xy| = |x||y|$, chaque fois que x et y sont des nombres réels. ▲

LEVERAGING PREUVE PAR CAS Les exemples que nous avons présentés illustrent la preuve par les cas donnent un aperçu de l'utilisation de cette méthode de preuve. En particulier, lorsqu'il n'est pas possible de considérer tous les cas d'une preuve en même temps, une preuve par cas doit être envisagée. Quand devez-vous utiliser une telle preuve? En règle générale, recherchez une preuve par cas lorsqu'il n'y a pas manière évidente de commencer une preuve, mais lorsque des informations supplémentaires dans chaque cas aident à déplacer la preuve vers l'avant. L'exemple 5 illustre comment la méthode de la preuve par cas peut être utilisée efficacement.

EXEMPLE 5 Formulez une conjecture sur le dernier chiffre décimal du carré d'un entier et prouvez votre résultat.

Solution: les plus petits carrés parfaits sont 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, etc. On remarque que les chiffres qui apparaissent comme le dernier chiffre d'un carré sont 0, 1, 4, 5, 6, et 9, avec 2, 3, 7, et 8 n'apparaissant comme étant le chiffre final d'un carré. Nous conjecturons ce théorème: Le dernier chiffre décimal d'un carré parfait est 0, 1, 4, 5, 6 ou 9. Comment pouvons-nous prouver ce théorème?

Nous notons d'abord que nous pouvons exprimer un entier n comme $10a + b$, où a et b sont pos-entiers itifs et b est 0, 1, 2, 3, 4, 5, 6, 7, 8 ou 9. Ici a est l'entier obtenu par en soustrayant le dernier chiffre décimal de n de n et en divisant par 10. Ensuite, notez que $(10a + b)^2 = 100a^2 + 20ab + b^2 = 10(10a^2 + 2b) + b^2$, de sorte que le dernier chiffre décimal de n^2 est le même que le dernier chiffre décimal de b^2. De plus, notez que le dernier chiffre décimal de b^2 est le même que le dernier chiffre décimal de $(10 - b)^2 = 100 - 20b + b^2$. Par conséquent, nous pouvons réduire notre preuve à l'examen de six cas.

Cas (i): Le dernier chiffre de n est 1 ou 9. Alors le dernier chiffre décimal de n^2 est le dernier chiffre chiffre de $1^2 = 1$ ou $9^2 = 81$, soit 1.

Cas (ii): Le dernier chiffre de n est 2 ou 8. Alors le dernier chiffre décimal de n^2 est le dernier chiffre chiffre de $2^2 = 4$ ou $8^2 = 64$, soit 4.

Cas (iii): Le dernier chiffre de n est 3 ou 7. Ensuite, le dernier chiffre décimal de n^2 est le dernier chiffre chiffre de $3^2 = 9$ ou $7^2 = 49$, soit 9.

Cas (iv): Le dernier chiffre de n est 4 ou 6. Ensuite, le dernier chiffre décimal de n^2 est le dernier chiffre chiffre de $4^2 = 16$ ou $6^2 = 36$, soit 6.

Cas (v): Le dernier chiffre décimal de n est 5. Alors le dernier chiffre décimal de n^2 est le dernier chiffre décimal de $5^2 = 25$, soit 5.

Cas (vi): Le dernier chiffre décimal de n est 0. Alors le dernier chiffre décimal de n^2 est le dernier chiffre décimal de $0^2 = 0$, à savoir 0.

Parce que nous avons considéré les six cas, nous pouvons conclure que le dernier chiffre décimal de n^2, où n est un entier vaut 0, 1, 2, 4, 5, 6 ou 9. ▲

Parfois, nous pouvons éliminer tous, sauf quelques exemples, dans une preuve par cas, comme l'exemple 6 illustre.

EXEMPLE 6 Montrer qu'il n'y a pas de solutions dans les entiers x et y de $x^2 + 3y^2 = 8$.

Solution: nous pouvons rapidement réduire une épreuve à la vérification de quelques cas simples car $x^2 > 8$ quand $|x| \geq 3$ et $3y^2 > 8$ lorsque $|y| \geq 2$. Cela laisse les cas où x est égal à -2, -1, 0, 1, ou 2 et y est égal à -1, 0 ou 1. Nous pouvons terminer en utilisant une preuve exhaustive. Pour se passer du cas restants, nous notons que les valeurs possibles pour x^2 sont 0, 1 et 4, et les valeurs possibles pour $3y^2$ sont 0 et 3, et la plus grande somme de valeurs possibles pour x^2 et $3y^2$ est 7. Par conséquent, il est impossible pour $x^2 + 3y^2 = 8$ de tenir lorsque x et y sont des entiers. ▲

SANS PERTE DE GÉNÉRALITÉ Dans la preuve de l'exemple 4, nous avons rejeté le cas (*iii*), où $x < 0$ et $y \geq 0$, car c'est la même chose que dans le cas (*ii*), où $x \geq 0$ et $y < 0$, avec le rôles de x et y inversés. Pour raccourcir la preuve, nous aurions pu prouver ensemble les cas (*ii*) et (*iii*) en supposant, **sans perte de généralité**, que $x \geq 0$ et $y < 0$. Implicite dans cette déclaration est que nous pouvons compléter le cas avec $x < 0$ et $y \geq 0$ en utilisant le même argument que nous avons utilisé pour le cas avec $x \geq 0$ et $y < 0$, mais avec les changements évidents.

En général, lorsque l'expression «sans perte de généralité» est utilisée dans une preuve (souvent abrégée comme WLOG), nous affirmons qu'en prouvant un cas de théorème, aucun argument supplémentaire n'est requis pour prouver d'autres cas spécifiés. Autrement dit, d'autres cas suivent en apportant des modifications simples à l'argument, ou en remplissant une étape initiale simple. Les preuves par cas peuvent souvent être rendu beaucoup plus efficace lorsque la notion de sans perte de généralité est employée. Bien sûr, une mauvaise utilisation de ce principe peut conduire à de malheureuses erreurs. Parfois, des hypothèses sont faites qui conduisent à une perte de généralité. Ces hypothèses peuvent être faites sans tenir compte qu'un cas peut être sensiblement différent des autres. Cela peut conduire à une éventuellement inaltérable, preuve. En fait, de nombreuses preuves incorrectes de théorèmes célèbres se sont avérées s'appuyer sur des arguments qui utilisaient l'idée de «sans perte de généralité» pour établir des cas n'a pas pu être rapidement prouvé à partir de cas plus simples.

Dans une preuve par cas être assurez-vous de n'omettre aucun cas et vérifiez que vous avez a prouvé tous les cas correctement!

Nous illustrons maintenant une preuve où sans perte de généralité est utilisé efficacement avec autres techniques de preuve.

EXEMPLE 7 Montrez que si x et y sont des entiers et que xy et $x + y$ sont pairs, alors x et y sont pairs.

Solution: Nous utiliserons la preuve par contraposition, la notion de sans perte de généralité et la preuve par cas. Supposons d'abord que x et y ne soient pas tous les deux pairs. Autrement dit, supposons que x est impair ou que y est impair (ou les deux). Sans perte de généralité, nous supposons que x est impair, de sorte que $x = 2m + 1$ pour certains entier k.

Pour compléter la preuve, nous devons montrer que xy est impair ou $x + y$ est impair. Considérer deux cas: (i) y pair et (ii) y impair. Dans (i), $y = 2n$ pour un entier n, de sorte que $x + y = (2m + 1) + 2n = 2(m + n) + 1$ est impair. Dans (ii), $y = 2n + 1$ pour un entier n, de sorte que $xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ est impair. Ceci termine la preuve par contraposition. (Notez que notre utilisation sans perte de généralité dans la preuve est justifié parce que la preuve lorsque y est impair peut être obtenue en échangeant simplement les rôles de x et y dans la preuve que nous avons donnée.) ▲

ERREURS COMMUNES ET AVEC LA PREUVE EXHAUSTIF preuve par cas un commun erreur de raisonnement est de tirer des conclusions incorrectes à partir d'exemples. Peu importe combien de séparer des exemples sont considérés, un théorème n'est pas prouvé en considérant des exemples à moins que

l'affaire est couverte. Le problème de prouver un théorème est analogue à montrer qu'un ordinateur programme produit toujours la sortie souhaitée. Peu importe le nombre de valeurs d'entrée testées, sauf toutes les valeurs d'entrée sont testées, nous ne pouvons pas conclure que le programme produit toujours la bonne production.

EXEMPLE 8 Est-il vrai que chaque entier positif est la somme de 18 quatrièmes puissances d'entiers?

Solution: Pour déterminer si un entier positif n peut être écrit comme la somme de 18 quatrièmes puissances d'entiers, nous pourrions commencer par examiner si n est la somme de 18 quatrièmes puissances d'entiers pour les plus petits entiers positifs. Parce que les quatrièmes puissances des entiers sont 0, 1, 16, 81, ..., si nous pouvons sélectionner 18 termes parmi ces nombres qui totalisent n, alors n est la somme de 18 quatrième pouvoirs. Nous pouvons montrer que tous les entiers positifs jusqu'à 78 peuvent être écrits comme la somme de 18 quatrième pouvoirs. (Les détails sont laissés au lecteur.) Cependant, si nous décidions que c'était assez de vérification, nous arriverions à une mauvaise conclusion. Il n'est pas vrai que chaque entier positif soit la somme de 18 quatrièmes pouvoirs parce que 79 n'est pas la somme de 18 quatrièmes pouvoirs (comme le lecteur peut le vérifier). ▲

Une autre erreur courante consiste à faire des hypothèses injustifiées qui conduisent à des erreurs preuves par cas où tous les cas ne sont pas pris en compte. Ceci est illustré dans l'exemple 9.

EXEMPLE 9 Quel est le problème avec cette «preuve»?

"Théorème:" Si x est un nombre réel, alors x^2 est un nombre réel positif.

"Preuve:" Soit p_1 soit " x est positif", soit p_2 soit " x est négatif", et soit q soit " x^2 est positif". montrer que $p_1 \to q$ est vrai, notez que lorsque x est positif, x^2 est positif car c'est le produit de deux nombres positifs, x et x. Pour montrer que $p_2 \to q$, notez que lorsque x est négatif, x^2 est positif car il est le produit de deux nombres négatifs, x et x. Ceci complète la preuve.

Solution: Le problème avec cette «preuve» est que nous avons raté le cas de $x = 0$. Lorsque $x = 0$, $x^2 = 0$ n'est pas positif, donc le théorème supposé est faux. Si p est « x est un nombre réel», alors nous pouvons prouver des résultats où p est l'hypothèse avec trois cas, p_1, p_2 et p_3, où

p_1 est « x est positif», p_2 est « x est négatif» et p_3 est « $x = 0$» en raison de l'équivalence $p \leftrightarrow p_1 \vee p_2 \vee p_3$. ▲

Preuves d'existence

De nombreux théorèmes sont des affirmations selon lesquelles des objets d'un type particulier existent. Un théorème de ce type est un proposition de la forme $\exists x P(x)$, où P est un prédicat. Une preuve d'une proposition de la forme $\exists x P(x)$ est appelé une **preuve d'existence** . Il existe plusieurs façons de prouver un théorème de ce type.

Parfois, une preuve d'existence de $\exists x P(x)$ peut être donnée en trouvant un élément a, appelé **témoin** , tel que $P(a)$ est vrai. Ce type de preuve d'existence est appelé **constructif** . Il est également possible donner une preuve d'existence **non constructive** ; qui est, nous ne trouvons pas un élément d' *un* tel que $P(a)$ est vrai, mais prouve plutôt que $\exists x P(x)$ est vrai d'une autre manière. Une méthode courante donner une preuve d'existence non constructive, c'est utiliser la preuve par contradiction et montrer que le la négation de la quantification existentielle implique une contradiction. Le concept de constructif la preuve d'existence est illustrée par l'exemple 10 et le concept d'une existence non constructive la preuve est illustrée par l'exemple 11.

EXEMPLE 10 **Une preuve d'existence constructive** Montrez qu'il existe un entier positif qui peut être écrit comme la somme des cubes d'entiers positifs de deux manières différentes.

Solution: Après un calcul considérable (comme une recherche informatique), nous constatons que

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$

Parce que nous avons affiché un entier positif qui peut être écrit comme la somme de cubes en deux de différentes manières, nous avons terminé.

Il y a une histoire intéressante concernant cet exemple. Le mathématicien anglais GH Hardy, en visitant le prodige indien malade Ramanujan à l'hôpital, a remarqué que 1729, le numéro du taxi qu'il prit était plutôt ennuyeux. Ramanujan a répondu: «Non, c'est très intéressant nombre; c'est le plus petit nombre exprimable comme la somme des cubes de deux manières différentes. » ▲

EXEMPLE 11 **Une preuve d'existence non constructive** Montrez qu'il existe des nombres irrationnels x et y tels que x^y est rationnel.

Solution: par l'exemple 10 de la section 1.7, nous savons que $\sqrt{2}$ est irrationnel. Considérez le nombre $\sqrt{2}^{\sqrt{2}}$. S'il est rationnel, nous avons deux nombres irrationnels x et y avec x^y rationnel, à savoir, $x = \sqrt{2}$ et $y = \sqrt{2}$. En revanche, si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, alors on peut laisser $x = \sqrt{2}^{\sqrt{2}}$ et $y = \sqrt{2}$ de sorte que $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = \sqrt{2}^2 = 2$.

Cette preuve est un exemple de preuve d'existence non constructive car nous n'avons pas trouvé nombres irrationnels x et y tels que x^y est rationnel. Nous avons plutôt montré que la paire $x = \sqrt{2}$, $y = \sqrt{2}$ ou la paire $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ ont la propriété souhaitée, mais nous ne savons pas laquelle de ces deux paires fonctionne! ▲

GODFREY HAROLD HARDY (1877-1947) Hardy, né à Cranleigh, Surrey, Angleterre, était l'aîné de deux enfants d'Isaac Hardy et Sophia Hall Hardy. Son père était maître de géographie et de dessin au Cranleigh School et a également donné des cours de chant et joué au football. Sa mère a donné des leçons de piano et a aidé gérer un pensionnat pour jeunes étudiants. Les parents de Hardy étaient dévoués à l'éducation de leurs enfants. Robuste a démontré sa capacité numérique à l'âge de deux ans quand il a commencé à écrire des nombres dans le des millions. Il avait un professeur de mathématiques privé plutôt que de suivre des cours réguliers à la Cranleigh School. Il a déménagé au Winchester College, une école secondaire privée, quand il avait 13 ans et a reçu une bourse. Il a excellé dans ses études et a démontré un fort intérêt pour les mathématiques. Il est entré au Trinity College de Cambridge en 1896 sur une bourse et a remporté plusieurs prix pendant son séjour là-bas, diplômé en 1899.

Hardy a occupé le poste de chargé de cours en mathématiques au Trinity College de l'Université de Cambridge de 1906 à 1919, alors qu'il était nommé à la chaire Sullivan de géométrie à Oxford. Il était devenu mécontent de Cambridge sur le licenciement du célèbre philosophe et mathématicien Bertrand Russell de Trinity pour les activités anti-guerre et n'a pas aimé une lourde charge administrative fonctions. En 1931, il est retourné à Cambridge en tant que professeur sadleirien de mathématiques pures, où il est resté jusqu'à sa retraite. en 1942. Il était un pur mathématicien et avait une vision élitiste des mathématiques, espérant que ses recherches ne pourraient jamais être appliquées. Ironiquement, il est peut-être mieux connu comme l'un des développeurs de la loi Hardy-Weinberg, qui prédit les modèles d'héritage. Son travail dans ce domaine est apparu sous forme de lettre à la revue *Science* dans laquelle il a utilisé des idées algébriques simples pour démontrer des erreurs dans un article sur la génétique. Hardy a travaillé principalement dans la théorie des nombres et la théorie des fonctions, explorant des sujets tels que la zêta de Riemann , série de Fourier et distribution des nombres premiers. Il a apporté de nombreuses contributions importantes à de nombreux problèmes importants, tels que comme le problème de Waring sur la représentation des entiers positifs comme des sommes de *k* ème puissances et le problème de la représentation des entiers impairs comme sommes de trois nombres premiers. On se souvient également de Hardy pour ses collaborations avec John E. Littlewood, un collègue de Cambridge, avec à qui il a écrit plus de 100 articles, et le célèbre prodige mathématique indien Srinivasa Ramanujan. Sa collaboration avec

Littlewood a conduit à la blague qu'il n'y avait que trois mathématiciens anglais importants à l'époque, Hardy, Littlewood et Hardy–Littlewood, bien que certaines personnes pensaient que Hardy avait inventé une personne fictive, Littlewood, parce que Littlewood était rarement vu à l'extérieur de Cambridge. Hardy avait la sagesse de reconnaître le génie de Ramanujan de non conventionnel mais extrêmement créatif les écrits que Ramanujan lui a envoyés, tandis que d'autres mathématiciens n'ont pas vu le génie. Hardy a amené Ramanujan à Cambridge et collaboré à d'importants articles communs, établissant de nouveaux résultats sur le nombre de partitions d'un entier. Hardy était intéressé dans l'enseignement des mathématiques, et son livre *Un cours de mathématiques pures a* eu un effet profond sur l'enseignement de premier cycle en mathématiques dans la première moitié du XXe siècle. Hardy a également écrit *les excuses d'un mathématicien* , dans lesquelles il donne sa réponse à la question de savoir s'il vaut la peine de consacrer sa vie à l'étude des mathématiques. Il présente le point de vue de Hardy sur ce les mathématiques et ce que fait un mathématicien.

Hardy avait un fort intérêt pour le sport. Il était un grand fan de cricket et suivait de près les scores. Un trait particulier qu'il avait était que il n'aimait pas sa photo prise (seulement cinq instantanés sont connus) et détestait les miroirs, les couvrant de serviettes immédiatement après entrer dans une chambre d'hôtel.

Les preuves d'existence non constructives sont souvent assez subtiles, comme l'illustre l'exemple 12.

EXEMPLE 12 **Chomp** est un jeu joué par deux joueurs. Dans ce jeu, les cookies sont disposés sur une grille rectangulaire. Le cookie en haut à gauche est empoisonné, comme le montre la figure 1 (a). Les deux joueurs prennent tourne en bougeant; à chaque coup, un joueur est tenu de manger un cookie restant, ainsi que tous les cookies à droite et / ou en dessous (voir la figure 1 (b), par exemple). Le perdant est le joueur qui n'a pas d'autre choix que de manger le cookie empoisonné. Nous demandons si l'un des deux joueurs a un stratégie gagnante. Autrement dit, l'un des joueurs peut-il toujours faire des mouvements qui sont garantis pour mener à une victoire?

Solution: Nous donnerons une preuve d'existence non constructive d'une stratégie gagnante pour la première joueur. Autrement dit, nous allons montrer que le premier joueur a toujours une stratégie gagnante sans explicitement décrivant les mouvements que ce joueur doit suivre.

Tout d'abord, notez que le jeu se termine et ne peut pas se terminer par un match nul car à chaque mouvement au moins un cookie est mangé, donc après pas plus de $m \times n$ déplace la fin du jeu, où la grille initiale est $m \times n$. Supposons maintenant que le premier joueur commence le jeu en ne mangeant que le cookie Le coin inférieur droit. Il y a deux possibilités, c'est le premier pas d'une stratégie gagnante pour le premier joueur, ou le deuxième joueur peut faire un coup qui est le premier coup d'une stratégie gagnante pour le deuxième joueur. Dans ce deuxième cas, au lieu de ne manger que le cookie en bas à droite coin, le premier joueur aurait pu faire le même coup que le deuxième joueur a fait comme le premier

SRINIVASA RAMANUJAN (1887–1920) Le célèbre prodige mathématique Ramanujan est né et a grandi dans le sud de l'Inde, près de la ville de Madras (maintenant appelée Chennai). Son père était commis dans un magasin de tissus. Sa mère contribué au revenu familial en chantant dans un temple local. Ramanujan a étudié à la langue anglaise locale l'école, montrant son talent et son intérêt pour les mathématiques. À l'âge de 13 ans, il maîtrise un manuel utilisé par étudiants. À l'âge de 15 ans, un étudiant lui a prêté une copie du *Synopsis of Pure Mathematics* . Ramanujan a décidé de travailler sur plus de 6000 résultats dans ce livre, a déclaré sans preuve ni explication, écrit sur des feuilles collectées plus tard pour former des cahiers. Il a obtenu son diplôme d'études secondaires en 1904, remportant une bourse Université de Madras. En s'inscrivant à un programme de beaux-arts, il a négligé ses matières autres que les mathématiques et a perdu sa bourse. Il n'a pas réussi les examens à l'université à quatre reprises de 1904 à 1907, réussissant bien uniquement en mathématiques. Pendant ce temps, il remplit ses cahiers d'écrits originaux, redécouvrant parfois déjà publiés travailler et à d'autres moments faire de nouvelles découvertes.

Sans diplôme universitaire, il était difficile pour Ramanujan de trouver un emploi décent. Pour survivre, il devait dépendre de la bonne volonté de ses amis. Il a enseigné aux élèves en mathématiques, mais ses façons de penser non conventionnelles et son incapacité à s'en tenir au programme ont causé problèmes. Il s'est marié en 1909 dans un mariage arrangé avec une jeune femme de neuf ans sa cadette. Besoin de subvenir à ses besoins et sa femme, il a déménagé à Madras et a cherché un emploi. Il a montré ses cahiers d'écrits mathématiques à ses employeurs potentiels, mais les livres les déroutaient. Cependant, un professeur du Presidency College a reconnu son génie et l'a soutenu, et en 1912 il a trouvé du travail comme commis aux comptes, gagnant un petit salaire.

Ramanujan a continué son travail mathématique pendant cette période et a publié son premier article en 1910 dans une revue indienne. Il a réalisé que son travail était au-delà de celui des mathématiciens indiens et a décidé d'écrire à d'éminents mathématiciens anglais. La première les mathématiciens auxquels il a écrit ont refusé sa demande d'aide. Mais en janvier 1913, il écrivit à GH Hardy, qui était enclin pour refuser Ramanujan, mais les déclarations mathématiques contenues dans la lettre, bien qu'énoncées sans preuve, intriguèrent Hardy. Il a décidé de les examiner de près avec l'aide de son collègue et collaborateur JE Littlewood. Ils ont décidé, après une étude approfondie, que Ramanujan était probablement un génie, car ses déclarations «ne pouvaient être écrites que par un mathématicien de la plus haute classe; elles doivent être vraies, car si elles ne l'étaient pas, personne n'aurait l'imagination pour les inventer. »

Hardy a organisé une bourse pour Ramanujan, l'amenant en Angleterre en 1914. Hardy l'a personnellement instruit en mathématiques analyse, et ils ont collaboré pendant cinq ans, ce qui prouve des théorèmes importants sur le nombre de partitions d'entiers. Pendant Ça temps, Ramanujan a apporté d'importantes contributions à la théorie des nombres et a également travaillé sur les fractions continues, les séries infinies et elliptiques les fonctions. Ramanujan avait une perspicacité étonnante impliquant certains types de fonctions et de séries, mais ses prétendus théorèmes sur le premier les chiffres étaient souvent erronés, illustrant sa vague idée de ce qui constitue une preuve correcte. Il était l'un des plus jeunes membres de l'histoire nommé membre de la Royal Society. Malheureusement, en 1917, Ramanujan est tombé extrêmement malade. À l'époque, on pensait qu'il avait des problèmes avec le climat anglais et avait contracté la tuberculose. On pense maintenant qu'il souffrait d'une carence en vitamines, provoquée par le strict végétarisme de Ramanujan et les pénuries en temps de guerre en Angleterre. Il est retourné en Inde en 1919, continuant à faire des mathématiques même lorsqu'il est confiné dans son lit. Il était religieux et pensait que son talent mathématique venait de sa divinité familiale, Namagiri. Il considérait que les mathématiques et la religion étaient liées. Il a dit que «pour moi, une équation n'a de sens que si elle exprime une pensée de Dieu. »Sa courte vie a pris fin en avril 1920, alors qu'il avait 32 ans. Ramanujan a laissé plusieurs cahiers de résultats non publiés. Les écrits dans ces cahiers illustrent les idées de Ramanujan mais sont assez sommaires. Plusieurs mathématiciens ont consacré de nombreuses années d'étude à expliquer et à justifier les résultats de ces cahiers.

(une) b)

FIGURE 1 **(a) Chomp (Cookie en haut à gauche empoisonné).(b) Trois mouvements possibles.**

mouvement d'une stratégie gagnante (et a ensuite continué à suivre cette stratégie gagnante). Ce serait garantir une victoire pour le premier joueur.

Notez que nous avons montré qu'une stratégie gagnante existe, mais nous n'avons pas spécifié de gain réel stratégie. Par conséquent, la preuve est une preuve d'existence non constructive.En fait, personne n'a été capable de décrire une stratégie gagnante pour ce Chomp qui s'applique à toutes les grilles rectangulaires par décrivant les mouvements que le premier joueur doit suivre.Cependant, les stratégies gagnantes peuvent être décrit pour certains cas particuliers, par exemple lorsque la grille est carrée et lorsque la grille n'a que deux rangées de cookies (voir les exercices 15 et 16 de la section 5.2). ▲

Preuves d'unicité

Certains théorèmes affirment l'existence d'un élément unique avec une propriété particulière.En d'autre En d'autres termes, ces théorèmes affirment qu'il existe exactement un élément avec cette propriété.Pour prouver un déclaration de ce type, nous devons montrer qu'un élément avec cette propriété existe et qu'aucun un autre élément a cette propriété. Les deux parties d'une **preuve d'unicité** sont:

Existence: Nous montrons qu'il existe un élément x avec la propriété souhaitée.
Unicité: Nous montrons que si $y = x$, alors y n'a pas la propriété souhaitée.

De manière équivalente, nous pouvons montrer que si x et y ont tous deux la propriété souhaitée, alors $x = y$.

Remarque: Montrer qu'il existe un élément unique x tel que $P(x)$ est le même que prouver le instruction $\exists x (P(x) \wedge \forall y (y = x \rightarrow \neg P(y)))$.

Nous illustrons les éléments d'une preuve d'unicité dans l'exemple 13.

EXEMPLE 13 Montrer que si a et b sont des nombres réels et $a = 0$, alors il existe un nombre réel unique r tel que $ar + b = 0$.

Solution: Tout d'abord, notez que le nombre réel $r = -b / a$ est une solution de $ar + b = 0$ car $a(-b/a) + b = -b + b = 0$. Par conséquent, il existe un nombre réel r pour lequel $ar + b = 0$. Ce est la partie existence de la preuve.

D' autre part, supposons que s est un nombre réel tel que *comme* $+ b = 0$. $ar + b =$ *comme* $+ b$, où $r = -b / a$. En soustrayant b des deux côtés, nous constatons que $ar = as$. Diviser les deux côtés de ce dernier équation par a , qui est non nulle, nous voyons que $r = s$. Cela signifie que si $s = r$, alors *comme* $+ b = 0$. Cela établit la partie unique de la preuve. ▲

Stratégies de preuve

Trouver des preuves peut être une entreprise difficile. Lorsque vous êtes confronté à une déclaration prouver, vous devez d'abord remplacer les termes par leurs définitions, puis analyser soigneusement hypothèses et la conclusion moyenne. Après cela, vous pouvez essayer de prouver le résultat en utilisant l'une des méthodes de preuve disponibles. En règle générale, si l'instruction est une instruction conditionnelle, vous devez d'abord essayer une preuve directe; si cela échoue, vous pouvez essayer une preuve indirecte. Si aucun de ces approche des travaux, vous pourriez essayer une preuve par contradiction.

RAISONNEMENT AVANT ET ARRIÈRE Quelle que soit la méthode choisie, vous avez besoin un point de départ pour votre preuve. Pour commencer une preuve directe d'une instruction conditionnelle, vous commencez avec les locaux. En utilisant ces prémisses, ainsi que des axiomes et des théorèmes connus, vous pouvez construire une preuve en utilisant une séquence d'étapes qui mène à la conclusion. Ce type de raisonnement, appelé *raisonnement avancé* , est le type de raisonnement le plus couramment utilisé pour prouver relativement simple résultats. De même, avec un raisonnement indirect, vous pouvez commencer par la négation de la conclusion et, en utilisant une séquence d'étapes, obtenir la négation des lieux.

Malheureusement, le raisonnement direct est souvent difficile à utiliser pour prouver des résultats plus compliqués, car le raisonnement nécessaire pour parvenir à la conclusion souhaitée peut être loin d'être évident Dans un tel Dans certains cas, il peut être utile d'utiliser le *raisonnement en arrière* . Pour raisonner en arrière pour prouver une déclaration q , nous trouvons une déclaration p que nous pouvons prouver avec la propriété que $p \to q$. (Notez que ce n'est pas utile trouver une déclaration r que vous pouvez prouver telle que $q \to r$, car c'est l'erreur de mendier la question de conclure de $q \to r$ et r que q est vrai.) Le raisonnement en arrière est illustré dans Exemples 14 et 15.

EXEMPLE 14 Etant donné deux nombres réels positifs x et y , leur **moyenne arithmétique** est $(x+y)/2$ et leur **géo-la moyenne métrique** est $\sqrt{xy}$. Lorsque nous comparons les moyennes arithmétiques et géométriques de paires de nombres réels positifs, nous constatons que la moyenne arithmétique est toujours supérieure à la géométrie signifier. [Par exemple, lorsque $x = 4$ et $y = 6$, nous avons $5 = (4+6)/2 > \sqrt{4 \cdot 6} = \sqrt{24}$.] Peut nous prouvons que cette inégalité est toujours vraie?

Solution: prouver que $(x+y)/2 > \sqrt{xy}$ lorsque x et y sont des nombres réels positifs distincts, nous pouvons travailler en arrière. Nous construisons une séquence d'inégalités équivalentes. L'équivalent les inégalités sont

$$(x+y)/2 > \sqrt{xy},$$

$$(x+y)^2/\text{quatre} > xy,$$

$$(x+y)^2 > 4xy,$$

$$x^2 + 2xy + y^2 > 4xy,$$

$$x^2 - 2xy + y^2 > 0,$$

$$(x-y)^2 > 0.$$

Parce que $(x-y)^2 > 0$ lorsque $x = y$, il s'ensuit que l'inégalité finale est vraie. Parce que tous ces les inégalités sont équivalentes, il s'ensuit que $(x+y)/2 > \sqrt{xy}$ lorsque $x = y$. Une fois que nous avons porté ce raisonnement en arrière, nous pouvons facilement inverser les étapes pour construire une preuve en utilisant avant raisonnement. Nous donnons maintenant cette preuve.

Supposons que x et y soient des nombres réels positifs distincts. Alors $(x-y)^2 > 0$ car le carré d'un nombre réel non nul est positif (voir annexe 1). Parce que $(x-y)^2 = x^2 - 2xy + y^2$, cela implique que $x^2 - 2xy + y^2 > 0$. En ajoutant $4xy$ des deux côtés, on obtient $x^2 + 2xy + y^2 > 4xy$. Parce que $x^2 + 2xy + y^2 = (x+y)^2$, cela signifie que $(x+y)^2 \geq 4xy$. En divisant les deux côtés de cette équation par 4, on voit que $(x+y)^{\text{deux}}/4 > xy$. Enfin, en prenant carré les racines des deux côtés (ce qui préserve l'inégalité parce que les deux côtés sont positifs) donne

$(x + y) / 2 > \sqrt{xy}$. Nous concluons que si x et y sont des nombres réels positifs distincts, alors leur moyenne arithmétique $(x + y) / 2$ est supérieure à leur moyenne géométrique $\sqrt{xy}$. ▲

EXEMPLE 15 Supposons que deux personnes jouent à un jeu à tour de rôle en retirant une, deux ou trois pierres à la fois à partir d'une pile qui commence par 15 pierres. La personne qui retire la dernière pierre gagne la partie. Montrez que le premier joueur peut gagner la partie, peu importe ce que fait le deuxième joueur.

Solution: Pour prouver que le premier joueur peut toujours gagner la partie, nous travaillons en arrière.Au dernière étape, le premier joueur peut gagner si ce joueur se retrouve avec une pile contenant un, deux ou trois des pierres. Le deuxième joueur sera obligé de laisser une, deux ou trois pierres si ce joueur doit retirer des pierres d'une pile contenant quatre pierres. Par conséquent, une façon pour la première personne de gagner consiste à laisser quatre pierres au deuxième joueur lors de l'avant-dernier mouvement.La première personne peut laissez quatre pierres lorsqu'il reste cinq, six ou sept pierres au début de la partie de ce joueur mouvement, qui se produit lorsque le deuxième joueur doit retirer des pierres d'une pile de huit pierres. Par conséquent, pour forcer le deuxième joueur à laisser cinq, six ou sept pierres, le premier joueur doit laisser huit pierres pour le deuxième joueur à l'avant-dernier coup pour le premier joueur.Ça signifie qu'il y a neuf, dix ou onze pierres lorsque le premier joueur fait ce mouvement.De même, le le premier joueur doit laisser douze pierres lorsque ce joueur fait le premier pas.Nous pouvons inverser cet argument pour montrer que le premier joueur peut toujours faire des mouvements pour que ce joueur gagne le jeu, peu importe ce que fait le deuxième joueur.Ces mouvements laissent successivement douze, huit et quatre pierres pour le deuxième joueur. ▲

ADAPTER LES **PREUVES EXISTANTES** Un excellent moyen de rechercher des approches possibles être utilisé pour prouver une déclaration est de tirer parti des preuves existantes de résultats similaires.Souvent une preuve existante peut être adaptée pour prouver d'autres faits.Même lorsque ce n'est pas le cas, certains les idées utilisées dans les épreuves existantes peuvent être utiles.Parce que les preuves existantes fournissent des indices pour de nouvelles preuves, vous devez lire et comprendre les preuves que vous rencontrez dans vos études.Ce processus est illustré dans l'exemple 16.

EXEMPLE 16 Dans l'exemple 10 de la section 1.7, nous avons prouvé que $\sqrt{2}$ est irrationnel. Nous conjecturons maintenant que $\sqrt{3}$ est irrationnel. Pouvons-nous adapter la preuve de l'exemple 10 de la section 1.7 pour montrer que 3 est irrationnel?

Solution: pour adapter la preuve de l'exemple 10 de la section 1.7, nous commençons par imiter les étapes de cette preuve, mais avec $\sqrt{2}$ remplacé par $\sqrt{3}$. Premièrement, nous supposons que $\sqrt{3} = d / c$ où la fraction c / d est en termes les plus bas. La quadrature des deux côtés nous dit que $3 = c^2 / d^2$, de sorte que $3 d^2 = c^2$. Peut-on utiliser cette équation pour montrer que 3 doit être un facteur à la fois c et d , semblable à la façon dont nous avons utilisé le équation $2 b^2 = a^2$ dans l'exemple 10 de la section 1.7 pour montrer que 2 doit être un facteur à la fois a et b ? (Rappelons qu'un entier s est un facteur de l'entier t si t / s est un entier. Un entier n est pair si et seulement si 2 est un facteur de n .) En fin de compte, nous pouvons, mais nous avons besoin de munitions de théorie des nombres, que nous développerons au chapitre 4. Nous esquissons le reste de la preuve, mais laissez la justification de ces étapes jusqu'au chapitre 4. Parce que 3 est un facteur de c^2 , il doit également être un facteur de c . De plus, comme 3 est un facteur de c , 9 est un facteur de c^2 , ce qui signifie que 9 est un facteur de $3 d^2$. Cela implique que 3 est un facteur de d^2 , ce qui signifie que 3 est un facteur de ce d . Cela fait de 3 un facteur à la fois c et d , ce qui contredit l'hypothèse selon laquelle c / d est au plus bas termes. Après avoir rempli la justification de ces étapes, nous aurons montré que $\sqrt{3}$ est irrationnel en adaptant la preuve que $\sqrt{2}$ est irrationnel. Notez que cette preuve peut être étendue à montre CA $\sqrt{n}$ est irrationnel chaque fois que n est un entier positif qui n'est pas un carré parfait.Nous partons les détails de cela au chapitre 4. ▲

Une bonne astuce consiste à rechercher des preuves existantes que vous pourriez adapter lorsque vous êtes confronté de prouver un nouveau théorème, en particulier lorsque le nouveau théorème semble similaire à celui que vous avez déjà prouvé.

Recherche de contre-exemples

Dans la section 1.7, nous avons introduit l'utilisation de contre-exemples pour montrer que certaines faux. Lorsque vous êtes confronté à une conjecture, vous pouvez d'abord essayer de prouver cette conjecture, et si vos tentatives ont échoué, vous pouvez essayer de trouver un contre-exemple, d'abord en regardant les exemples les plus simples et les plus petits.Si vous ne trouvez pas de contre-exemple, vous pouvez essayer à nouveau prouver la déclaration. Dans tous les cas, la recherche de contre-exemples est une activité extrêmement importante, qui donne souvent un aperçu des problèmes. Nous illustrerons le rôle des contre-exemples dans Exemple 17.

EXEMPLE 17 Dans l'exemple 14 de la section 1.7, nous avons montré que l'énoncé «Chaque entier positif est la somme de deux carrés d'entiers »est faux en trouvant un contre-exemple.Autrement dit, il y a des entiers positifs cela ne peut pas être écrit comme la somme des carrés de deux entiersBien que nous ne puissions pas écrire tous les entier positif comme la somme des carrés de deux entiers, peut-être pouvons-nous écrire chaque positif entier comme la somme des carrés de trois entiers. Autrement dit, est la déclaration «Chaque positif entier est la somme des carrés de trois entiers "vrai ou faux?

Solution: parce que nous savons que tous les entiers positifs ne peuvent pas être écrits comme la somme de deux carrés d'entiers, nous pourrions être sceptiques au départ que chaque entier positif peut être écrit comme la somme de trois carrés d'entiers. Donc, nous cherchons d'abord un contre-exemple. Autrement dit, nous pouvons montrer que l'énoncé «Chaque entier positif est la somme de trois carrés d'entiers» est faux si nous pouvons trouver un entier particulier qui n'est pas la somme des carrés de trois entiers.Regarder pour un contre-exemple, nous essayons d'écrire des entiers positifs successifs comme une somme de trois carrés. On constate que $1 = 0^2 + 0^2 + 1^2$, $2 = 0^2 + 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $4 = 0^2 + 0^2 + 2^2$, $5 = 0^2 + 1^2 + 2^2$, $6 = 1^2 + 1^2 + 2^2$, mais nous ne pouvons pas trouver un moyen d'écrire 7 comme la somme de trois carrés. Pour montrer qu'il n'y a pas trois carrés qui totalisent 7, on note que le seul possible les carrés que nous pouvons utiliser sont ceux ne dépassant pas 7, à savoir, 0, 1 et 4. Parce qu'il n'y a pas trois termes où chaque terme est égal à 0, 1 ou 4 totalisant 7, il s'ensuit que 7 est un contre-exemple. Nous concluons que le la déclaration «Chaque entier positif est la somme des carrés de trois entiers» est fausse.

Nous avons montré que tous les entiers positifs ne sont pas la somme des carrés de trois entiers. La prochaine question à se poser est de savoir si chaque entier positif est la somme des carrés de quatre entiers positifs. Certaines expérimentations prouvent que la réponse est oui.Par exemple, $7 = 1^2 + 1^2 + 1^2 + 2^2$, $25 = 4^2 + 2^2 + 2^2 + 1^2$ et $87 = 9^2 + 2^2 + 1^2 + 1^2$. Il s'avère que le la conjecture "Chaque entier positif est la somme des carrés de quatre entiers" est vraiePour une preuve, voir [Ro10]. ▲

Stratégie de preuve en action

Les mathématiques sont généralement enseignées comme si des faits mathématiques étaient gravés dans la pierre.Mathématiques les textes (y compris la majeure partie de ce livre) présentent formellement les théorèmes et leurs preuvesCette présence ne transmettent pas le processus de découverte en mathématiques.Ce processus commence par l'exploration concepts et exemples, poser des questions, formuler des conjectures, et tenter de régler ces conjectures soit par preuve soit par contre-exemple. Ce sont les activités quotidiennes des ématiciens. Croyez-le ou non, le matériel enseigné dans les manuels a été développé à l'origine dans ce façon.

Les gens formulent des conjectures sur la base de nombreux types de preuves possibles.L'examen- l'ination de cas particuliers peut conduire à une conjecture, de même que l'identification de schémas possibles. La modification des hypothèses et des conclusions des théorèmes connus peut également conduire à une conjonction plausible. tures. À d'autres moments, des conjectures sont faites sur la base de l'intuition ou de la conviction qu'un résultat est valable. Peu importe comment une conjecture a été faite, une fois formulée, le but est de prouver ou le réfuter. Lorsque les mathématiciens croient qu'une conjecture peut être vraie, ils essaient de trouver une preuve. S'ils ne trouvent pas de preuve, ils peuvent chercher un contre-exemple.Quand ils ne trouvent pas de pays Par exemple, ils peuvent changer de vitesse et essayer à nouveau de prouver la conjectureBien que beaucoup les conjectures sont rapidement réglées, quelques conjectures résistent à l'attaque pendant des centaines d'années et conduisent à

FIGURE 2 **Le damier standard.**

FIGURE 3
Deux dominos.

le développement de nouvelles parties des mathématiques.Nous mentionnerons quelques conjectures célèbres plus tard dans cette section.

Carrelages

Nous pouvons illustrer les aspects de la stratégie de preuve à travers une brève étude des pavages de damiers. Regarder les pavages de damiers est une façon fructueuse de découvrir rapidement de nombreux résultats différents et construire leurs preuves en utilisant une variété de méthodes de preuve.Il y a presque un nombre infini des conjectures qui peuvent être faites et étudiées dans ce domaine aussi.Pour commencer, nous devons définir certains termes. Un **damier** est un rectangle divisé en carrés de la même taille par horizontal et lignes verticales. Le jeu de dames se joue sur un plateau de 8 lignes et 8 colonnes;cette est appelé **damier standard** et est illustré à la figure 2. Dans cette section, nous utilisons le **panneau de** termes pour désigner un damier de toute taille rectangulaire ainsi que des parties de damiers obtenu en supprimant un ou plusieurs carrés.Un **domino** est une pièce rectangulaire qui est un carré par deux carrés, comme le montre la figure 3. Nous disons qu'une planche est **carrelée** par des dominos lorsque tous ses les carrés sont couverts sans dominos superposés et sans dominos surplombant la planche.nous développer maintenant quelques résultats sur les panneaux de carrelage utilisant des dominos.

EXEMPLE 18 Peut-on carreler le damier standard à l'aide de dominos?

Solution: Nous pouvons trouver de nombreuses façons de carreler le damier standard à l'aide de dominos.Par exemple, nous pouvons le carreler en plaçant 32 dominos horizontalement, comme le montre la figure 4. L'existence d'un un tel carrelage complète une preuve d'existence constructive. Bien sûr, il existe un grand nombre d'autres façons de faire ce carrelage. On peut placer 32 dominos verticalement sur la planche ou on peut en placer tuiles verticalement et certains horizontalement. Mais pour une preuve d'existence constructive, nous devions trouver juste un tel carrelage. ▲

EXEMPLE 19 Pouvons-nous carreler une planche obtenue en retirant l'un des quatre carrés d'angle d'un damier standard - planche?

Solution: pour répondre à cette question, notez qu'un damier standard a 64 carrés, donc la suppression un carré produit une planche de 63 carrés. Supposons maintenant que nous puissions carreler une planche obtenue du damier standard en supprimant un carré d'angle.Le conseil a un nombre pair de

FIGURE 4 **Mosaïque du damier standard.**

FIGURE 5 **Le damier standard avec le coin supérieur gauche et inférieur droit Carrés supprimés.**

carrés parce que chaque domino couvre deux carrés et pas deux dominos se chevauchent et pas de dominos surplombe la planche. Par conséquent, nous pouvons prouver par contradiction qu'un damier standard avec un carré retiré ne peut pas être carrelé à l'aide de dominos car une telle planche a une nombre de carrés. ▲

Nous considérons maintenant une situation plus délicate.

EXEMPLE 20 Peut-on carreler la planche obtenue en supprimant les coins supérieurs gauche et inférieur droit d'un damier standard, illustré à la figure 5?

Solution: un tableau obtenu en supprimant deux carrés d'un damier standard contient 64-2 = 62 carrés. Parce que 62 est pair, nous ne pouvons pas rapidement exclure l'existence d'un pavage de le damier standard avec ses carrés supérieur gauche et inférieur droit supprimés, contrairement à l'exemple 19, où nous avons exclu l'existence d'un carrelage du damier standard avec un coin carré supprimé. Essayer de construire un pavage de cette planche en plaçant successivement des dominos pourrait être une première approche, comme le lecteur devrait essayer.Cependant, peu importe combien nous essayons, nous ne pouvons pas trouver un tel carrelage. Parce que nos efforts ne produisent pas de carrelage, nous sommes amenés à des conjectures qu'aucun carrelage n'existe.

Nous pourrions essayer de prouver qu'il n'y a pas de carrelage en montrant que nous atteignons une impasse cependant nous plaçons successivement des dominos sur le plateau. Pour construire une telle preuve, il faudrait considérer tous les cas possibles qui surviennent alors que nous parcourons tous les choix possibles de placer des dominos. Par exemple, nous avons deux choix pour couvrir le carré dans le second colonne de la première ligne, à côté du coin supérieur gauche supprimé.On pourrait le recouvrir horizontalement tuile placée ou une tuile placée verticalement. Chacun de ces deux choix conduit à d'autres choix, et ainsi sur. Il ne faut pas longtemps pour voir que ce n'est pas un plan d'attaque fructueux pour une personne, bien qu'un ordinateur pourrait être utilisé pour compléter une telle preuve par épuisement.(L'exercice 45 vous demande de fournir une telle preuve pour montrer qu'un damier 4 × 4 avec des coins opposés retirés ne peut pas être carrelé.)

Nous avons besoin d'une autre approche. Peut-être existe-t-il un moyen plus simple de prouver qu'il n'existe pas damier standard avec deux coins opposés enlevés. Comme pour de nombreuses preuves, une observation clé les vacances peuvent aider. Nous colorons les carrés de ce damier en alternant le blanc et le noir carrés, comme dans la figure 2. Observez qu'un domino dans un carrelage d'une telle planche couvre un carré blanc et un carré noir. Ensuite, notez que cette carte a des nombres inégaux de carrés blancs et noirs

carrés. On peut utiliser ces observations pour prouver par contradiction qu'un damier standard avec les coins opposés enlevés ne peut pas être carrelé avec des dominosNous présentons maintenant une telle preuve.

Preuve: supposons que nous pouvons utiliser des dominos pour carreler un damier standard avec des coins opposés supprimé. Notez que le damier standard avec les coins opposés supprimés contient 64 - 2 = 62 carrés. Le carrelage utiliserait 62 / 2 = 31 Dominos. Notez que chaque domino de ce carrelage couvre un carré blanc et un carré noir. Par conséquent, le carrelage couvre 31 carrés blancs et 31 noirs carrés. Cependant, lorsque nous supprimons deux coins opposés, soit 32 des autres les carrés sont blancs et 30 sont noirs ou bien 30 sont blancs et 32 sont noirs.Cela contredit la hypothèse que nous pouvons utiliser des dominos pour couvrir un damier standard avec des coins opposés retiré, complétant la preuve. ▲

Nous pouvons utiliser d'autres types de pièces en plus des dominos dans les carrelages.Au lieu de dominos, nous pouvons étudier les pavages qui utilisent des pièces de forme identique construites à partir de carrés congrus qui sont connectés le long de leurs bords.Ces pièces sont appelées **polyominos** , un terme inventé en 1953 par le mathématicien Solomon Golomb, l'auteur d'un livre divertissant à leur sujet [Go94].nous considérera deux polyominos avec le même nombre de carrés identiques si nous pouvons tourner et / ou retournez l'un des polyominos pour obtenir l'autre.Par exemple, il existe deux types de triominos (voir figure 6), qui sont des polyominos composés de trois carrés reliés par leurs côtés.Un le type de triomino, le**triomino droit** , a trois carrés connectés horizontalement; L'autre type, **triominos droits** , ressemble à la lettre L en forme, retournée et / ou tournée, si nécessaire.nous étudiera ici les pavages d'un damier par des triominos droits;nous étudierons les carrelages par triominos droits dans la section 5.1.

FIGURE 6 **A Triomino droit et un droit Triomino.**

EXEMPLE 21 Pouvez-vous utiliser des triominos droits pour carreler un damier standard?

Solution: le damier standard contient 64 carrés et chaque triomino couvre trois carrés. Par conséquent, si les triominos tuiles une planche, le nombre de cases de la planche doit être un multiple de 3. Parce que 64 n'est pas un multiple de 3, les triominos ne peuvent pas être utilisés pour couvrir un 8 × 8 damier. ▲

Dans l'exemple 22, nous considérons le problème de l'utilisation de triominos droits pour paver une norme damier avec un coin manquant.

EXEMPLE 22 Peut-on utiliser des triominos droits pour carreler un damier standard avec l'un de ses quatre coins supprimé? Un damier 8 × 8 avec un coin retiré contient 64 - 1 = 63 carrés.Tout carrelage par Triomino droites de l' un de ces quatre planches utilise 63 / 3 = 21 Triomino. cependant, lorsque nous expérimentons, nous ne pouvons pas trouver un carrelage de l'une de ces planches en utilisant des triominos droits. Une preuve par épuisement ne semble pas prometteuse. Pouvons-nous adapter notre preuve de l'exemple 20 à prouver qu'aucun tel carrelage n'existe?

Solution: Nous colorerons les carrés du damier pour tenter d'adapter l'épreuve en

contradiction que nous avons donné dans l'exemple 20 de l'impossibilité d'utiliser des dominos pour carreler un standard
damier avec coins opposés enlevés. Parce que nous utilisons plutôt des triominos droits
que les dominos, nous colorons les carrés en utilisant trois couleurs plutôt que deux couleurs, comme indiqué dans
Figure 7. Notez qu'il y a 21 carrés bleus, 21 carrés noirs et 22 carrés blancs dans ce
coloration. Ensuite, nous faisons l'observation cruciale que lorsqu'un triomino droit couvre trois
carrés du damier, il couvre un carré bleu, un carré noir et un carré blanc.
Notez ensuite que chacune des trois couleurs apparaît dans un carré d'angle. Ainsi sans perte de généralité,
nous pouvons supposer que nous avons fait pivoter la coloration de sorte que le carré manquant soit coloré en bleu.
Par conséquent, nous supposons que le tableau restant contient 20 carrés bleus, 21 carrés noirs et
22 carrés blancs.

Si nous pouvions carreler cette planche en utilisant des triominos droits, alors nous utiliserions 63/3 = 21 droites
triominos. Ces triominos couvriraient 21 carrés bleus, 21 carrés noirs et 21 blancs

**FIGURE 7 Coloration des carrés du damier standard
avec trois couleurs.**

carrés. Cela contredit le fait que cette carte contient 20 carrés bleus, 21 carrés noirs et
22 carrés blancs. Par conséquent, nous ne pouvons pas carreler ce panneau en utilisant des triominos droits. ▲

Le rôle des problèmes ouverts

De nombreuses avancées en mathématiques ont été faites par des personnes essayant de résoudre des problèmes non résolus
problèmes. Au cours des 20 dernières années, de nombreux problèmes non résolus ont finalement été résolus, tels que
preuve d'une conjecture en théorie des nombres faite il y a plus de 300 ans. Cette conjecture affirme
la vérité de la déclaration connue comme **le dernier théorème de Fermat** .

THÉORÈME 1 **LE DERNIER THÉORÈME DE FERMAT** L'équation

$$x^n + y^n = z^n$$

n'a pas de solutions dans les entiers x , y et z avec $xyz = 0$ chaque fois que n est un entier avec $n > 2$.

Remarque: L'équation $x^2 + y^2 = z^2$ a une infinité de solutions en entiers x , y et z ; celles-ci
les solutions sont appelées triplets de Pythagore et correspondent aux longueurs des côtés de droite
triangles de longueurs entières. Voir l'exercice 32.

Ce problème a une histoire fascinante. Au XVIIe siècle, Fermat griffonne dans le
marge de sa copie des œuvres de Diophantus qu'il avait une "merveilleuse preuve" qu'il n'y a pas
solutions entières de $x^n + y^n = z^n$ lorsque n est un entier supérieur à 2 avec $xyz = 0$. Cependant,
il n'a jamais publié de preuve (Fermat n'a presque rien publié), et aucune preuve n'a pu être trouvée dans
les papiers qu'il a laissés à sa mort. Les mathématiciens ont cherché une preuve pendant trois siècles sans
succès, même si de nombreuses personnes étaient convaincues qu'une preuve relativement simple pouvait être trouvée.
(Des preuves de cas spéciaux ont été trouvées, telles que la preuve du cas lorsque $n = 3$ par Euler et le
preuve du cas $n = 4$ par Fermat lui-même.) Au fil des ans, plusieurs mathématiciens confirmés
pensaient qu'ils avaient prouvé ce théorème. Au XIXe siècle, l'une de ces tentatives infructueuses
conduit au développement de la partie de la théorie des nombres appelée théorie des nombres algébriques. Un correct

preuve, nécessitant des centaines de pages de mathématiques avancées, n'a été trouvée que dans les années 1990, quand Andrew Wiles a utilisé des idées récemment développées dans un domaine sophistiqué de la théorie des nombres appelé la théorie des courbes elliptiques pour prouver le dernier théorème de Fermat.La quête de Wiles pour trouver un preuve du dernier théorème de Fermat utilisant cette puissante théorie, décrite dans un programme du*Nova* série télévisée publique, a duré près de dix ans! De plus, sa preuve était fondée sur des contributions de nombreux mathématiciens. (Le lecteur intéressé devrait consulter [Ro10] pour plus des informations sur le dernier théorème de Fermat et pour des références supplémentaires concernant ce problème et sa résolution.)

Nous présentons maintenant un problème ouvert qui est simple à décrire, mais qui semble assez difficile à résoudre.

EXEMPLE 23 ***La conjecture* 3 *x* + 1** Soit T la transformation qui envoie un entier pair x à $x / 2$ et un entier impair x à $3x + 1$. Une conjecture célèbre, parfois appelée **conjonction 3 *x* + 1 ture** , déclare que pour tous les entiers positifs$x$, lorsque nous appliquons à plusieurs reprises la transformation$T$, nous atteindrons finalement l'entier 1. Par exemple, en commençant par$x = 13$, nous trouvons $T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$, $T(10) = 10/2 = 5$, $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 8$, $T(8) = 4$, $T(4) = 2$ et $T(2) = 1$. La conjecture $3x + 1$ a été vérifié en utilisant des ordinateurs pour tous les entiers$x$ jusqu'à $5 . 6 \cdot 10^{13}$.

La conjecture $3x + 1$ a une histoire intéressante et a attiré l'attention des mathématiciens depuis les années 50. La conjecture a été soulevée à plusieurs reprises et passe par de nombreuses autres noms, y compris le problème de Collatz, l'algorithme de Hasse, le problème d'Ulam, le problème de Syracuse lem, et le problème de Kakutani. De nombreux mathématiciens ont été détournés de leur travail pour passer le temps d'attaquer cette conjecture. Cela a conduit à la blague que ce problème faisait partie d'une conspiration pour ralentir la recherche mathématique américaine. Voir l'article de Jeffrey Lagarias [La10] pour un discussion fascinante sur ce problème et les résultats qui ont été trouvés par les mathématiciens l'attaquer. ▲

Fais attention! Travaille sur le problème $3x + 1$ peut être addictif.

Dans le chapitre 4, nous décrirons d'autres questions ouvertes sur les nombres premiers. Étudiants déjà familier avec les notions de base sur les nombres premiers pourrait vouloir explorer la section 4.3, où ces questions ouvertes sont discutées. Nous mentionnerons d'autres questions ouvertes importantes tout au long le livre.

Méthodes de preuve supplémentaires

Construisez votre arsenal de méthodes de preuve que vous travailler à travers ce livre.

Dans ce chapitre, nous avons présenté les méthodes de base utilisées dans les preuves. Nous avons également décrit comment tirer parti ces méthodes pour prouver une variété de résultats. Nous utiliserons ces méthodes de preuve dans toutes les chapitres. En particulier, nous les utiliserons dans les chapitres 2, 3 et 4 pour prouver les résultats sur les ensembles, fonctions, algorithmes et théorie des nombres et dans les chapitres 9, 10 et 11 pour prouver les résultats dans le graphique théorie. Parmi les théorèmes que nous allons prouver est le célèbre théorème d'arrêt qui déclare qu'il est un problème qui ne peut être résolu par aucune procédure. Cependant, il existe de nombreux méthodes de preuve en plus de celles que nous avons couvertes. Nous présenterons certaines de ces méthodes plus tard dans ce livre. En particulier, dans la section 5.1, nous discuterons de l'induction mathématique, qui est un méthode extrêmement utile pour prouver des déclarations de la forme $\forall n P(n)$, où le domaine se compose de tous les entiers positifs. Dans la section 5.3, nous introduirons l'induction structurelle, qui peut être utilisée pour prouver les résultats sur des ensembles définis récursivement. Nous utiliserons la méthode de diagonalisation de Cantor, qui peut être utilisé pour prouver les résultats sur la taille des ensembles infinis, dans la section 2.5Au chapitre 6 nous introduirons la notion de preuves combinatoires, qui peut être utilisée pour prouver les résultats par compter les arguments. Le lecteur doit noter que des livres entiers ont été consacrés aux activités discuté dans cette section, y compris de nombreuses excellentes œuvres de George Pólya ([Po61], [Po71], [Po90]).

Enfin, notons que nous n'avons pas donné de procédure pouvant être utilisée pour prouver des théorèmes dans mathématiques. C'est un théorème profond de la logique mathématique qu'il n'y a pas une telle procédure.

Des exercices

1. Montrer que $n^2 + 1 \geq 2^n$ quand n est un entier positif avec $1 \leq n \leq 4$.

2. Montrer qu'il n'y a pas de cubes parfaits positifs inférieurs à 1000 qui sont la somme des cubes de deux entiers positifs.

3. Montrer que si x et y sont des nombres réels, alors $\max(x, y) + \min(x, y) = x + y$. [*Astuce:* utilisez une preuve par cas, avec les deux cas correspondant à $x \geq y$ et $x < y$, respectivement activement.]

4. Utilisez une preuve par cas pour montrer que $\min(a, \min(b, c)) = \min(\min(a, b), c)$ chaque fois *que* a, b et c sont des nombres réels.

5. Prouver en utilisant la notion de sans perte de généralité que $\min(x, y) = (x + y - |x - y|)/2$ et $\max(x, y) = (x + y + |x - y|)/2$ lorsque x et y sont des nombres réels.

6. Prouver en utilisant la notion sans perte de généralité que $5x + 5y$ est un entier impair lorsque x et y sont des entiers de parité opposée.

7. Démontrez l' **inégalité** du **triangle** , qui stipule que si x et y sont des nombres réels, alors $|x| + |y| \geq |x + y|$ (où $|x|$ représente la valeur absolue de x, qui est égale à x si $x \geq 0$ et est égal à $-x$ si $x < 0$).

8. Démontrer qu'il existe un entier positif égal à la somme des entiers positifs ne le dépassant pas. Est votre preuve constructif ou non constructif?

9. Démontrer qu'il y a 100 entiers positifs consécutifs qui ne sont pas des carrés parfaits. Votre preuve est-elle constructive ou non constructif?

10. Démontrez que $2 \cdot 10^{500} + 15$ ou $2 \cdot 10^{500} + 16$ n'est pas un un carré parfait. Votre preuve est-elle constructive ou non tive?

11. Démontrer qu'il existe une paire d'entiers consécutifs tels que que l'un de ces nombres entiers est un carré parfait et l'autre est un cube parfait.

12. Montrer que le produit de deux des nombres $65^{1000} - 8^{2001} + 3^{177}$, $79^{1212} - 9^{2399} + 2^{2001}$ et $24^{4493} - 5^{8192} + 7^{1777}$ est non négatif. Votre preuve est-elle constructive ou non constructif? [*Astuce:* N'essayez pas d'évaluer ces Nombres!]

13. Démontrer ou infirmer qu'il existe un nombre rationnel x et un nombre irrationnel y tel que x^y est irrationnel.

14. Prouver ou infirmer que si a et b sont des nombres rationnels, puis a^b est également rationnel.

15. Montrer que chacune de ces déclarations peut être utilisée pour appuyez sur le fait qu'il existe un élément unique x tel que $P(x)$ est vrai. [Notez que nous pouvons également écrire cette déclaration comme $\exists! x P(x)$.]

a) $\exists x \forall y (P(y) \leftrightarrow x = y)$

b) $\exists x P(x) \land \forall x \forall y (P(x) \land P(y) \rightarrow x = y)$

c) $\exists x (P(x) \land \forall y (P(y) \rightarrow x = y))$

16. Montrez que si a, b et c sont des nombres réels et $a = 0$, alors il existe une solution unique de l'équation $ax + b = c$.

17. Supposons que a et b soient des entiers impairs avec $a = b$. Spectacle il existe un entier unique c tel que $|a - c| = |b - c|$.

18. Montrer que si r est un nombre irrationnel, il y a un unique entier n tel que la distance entre r et n soit inférieure à 1 / deux.

19. Montrer que si n est un entier impair, alors il y a un unique entier k tel que n est la somme de $k - 2$ et $k + 3$.

20. Montrer que, étant donné un nombre réel x, il existe un nombre unique bers n et ϵ tels que $x = n + \epsilon$, n est un entier, et $0 \leq \epsilon < 1$.

21. Montrer que, étant donné un nombre réel x, il existe un nombre unique bers n et ϵ tels que $x = n - \epsilon$, n est un entier, et $0 \leq \epsilon < 1$.

22. Utilisez le raisonnement direct pour montrer que si x est un réel non nul nombre, puis $x^2 + 1/x^2 \geq 2$. [*Astuce:* Commencez par égalité $(x - 1/x)^2 \geq 0$ qui vaut pour tout réel non nul nombres x .]

23. La **moyenne harmonique** de deux nombres réels x et y est égal $2xy/(x + y)$. En calculant l'harmonique et la géométrie au moyen de différentes paires de nombres réels positifs, tard une conjecture sur leurs tailles relatives et prouver votre conjecture.

24. La **moyenne quadratique** de deux nombres réels x et y équivaut à $(x^2 + y^2)/2$. En calculant l'arithmétique et moyennes quadratiques de différentes paires de nombres réels positifs bers, formuler une conjecture sur leurs tailles relatives et prouver votre conjecture.

∗ **25.** Écrivez les nombres $1, 2, \ldots, 2n$ sur un tableau noir, où n est un entier impair. Choisissez deux des nombres, j et k, écris $|j - k|$ sur le tableau et effacez j et k. Continuer ce processus jusqu'à ce qu'un seul entier soit écrit sur le tableau. Démontrez que cet entier doit être impair.

∗ **26.** Supposons que cinq uns et quatre zéros soient disposés autour un cercle. Entre deux bits égaux, vous insérez un 0 et entre deux bits inégaux, vous insérez un 1 pour produire neuf nouveaux bits. Ensuite, vous effacez les neuf bits d'origine. Spectacle que lorsque vous répétez cette procédure, vous ne pouvez jamais obtenir neuf zéros. [*Astuce:* travailler en arrière, en supposant que vous l'avez fait finir avec neuf zéros.]

27. Formulez une conjecture sur les chiffres décimaux qui poire comme le dernier chiffre décimal de la quatrième puissance d'un entier. Prouvez votre conjecture en utilisant une preuve par cas.

28. Formuler une conjecture sur les deux derniers chiffres décimaux du carré d'un entier. Prouvez votre conjecture en utilisant un preuve par cas.

29. Démontrer qu'il n'y a pas d'entier positif n tel que $n^2 + n^3 = 100$.

30. Démontrer qu'il n'y a pas de solution dans les entiers x et y à la équation $2x^2 + 5y^2 = 14$.

31. Montrer qu'il n'y a pas de solution dans les entiers positifs x et y à l'équation $x^4 + y^4 = 625$.

32. Prouver qu'il existe une infinité de solutions dans la posi- nombres entiers x, y et z à l'équation $x^2 + y^2 = z^2$. [*Astuce:* Soit $x = m^2 - n^2$, $y = 2mn$, et $z = m^2 + n^2$, où m et n sont des nombres entiers.]

33. Adapter la preuve de l'exemple 4 de la section 1.7 pour prouver que si $n = abc$, où a, b et c sont des entiers positifs, alors $a \le \sqrt[3]{n}$, $b \le \sqrt[3]{n}$, ou $c \le \sqrt[3]{n}$.

34. Prouver que $\sqrt[3]{2}$ est irrationnel.

35. Montrer qu'entre deux nombres rationnels, il y a un nombre irrationnel.

36. Montrer qu'entre chaque nombre rationnel et chaque irra- numéro national il y a un numéro irrationnel.

∗ **37.** Soit $S = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$, où $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_n$ sont des ordonnances de deux de nombres réels positifs, contenant chacun n éléments ments.

a) Montrer que S prend sa valeur maximale sur toutes les commandes des deux séquences lorsque les deux séquences sont triés (de sorte que les éléments de chaque séquence soient ordre non décroissant).

b) Montrer que S prend sa valeur minimale sur toute commande- des deux séquences lorsqu'une séquence est triée en ordre non décroissant et l'autre est trié en ordre non croissant.

38. Prouvez ou réfutez que si vous avez une cruche de 8 gallons d'eau ter et deux cruches vides avec des capacités de 5 gallons et 3 gallons, respectivement, alors vous pouvez mesurer 4 gallons par verser successivement une partie ou la totalité de l'eau dans une cruche dans une autre cruche.

39. Vérifiez la conjecture $3x + 1$ pour ces nombres entiers.

a) 6 **b)** 7 **c)** 17 **d)** 21

40. Vérifiez la conjecture $3x + 1$ pour ces nombres entiers.

a) 16 **b)** 11 **c)** 35 **d)** 113

41. Prouvez ou réfutez que vous pouvez utiliser des dominos pour carreler le damier standard avec deux coins adjacents déplacé (c'est-à-dire des coins qui ne sont pas opposés).

42. Prouvez ou réfutez que vous pouvez utiliser des dominos pour damier standard avec les quatre coins supprimés.

43. Prouvez que vous pouvez utiliser des dominos pour carreler un rectangle damier avec un nombre pair de carrés.

44. Prouvez ou réfutez que vous pouvez utiliser des dominos pour Damier 5×5 avec trois coins retirés.

45. Utilisez une preuve d'épuisement pour montrer qu'un carrelage utilisant dominos d'un damier 4×4 avec coins opposés supprimé n'existe pas. [*Indice:* montrez d'abord que vous pouvez supposons que les carrés en haut à gauche et en bas à droite les coins sont supprimés. Numéroter les carrés de l'original en damier de 1 à 16, à partir de la première rangée, à droite dans cette rangée, puis en commençant dans le carré le plus à gauche dans la deuxième rangée et en se déplaçant à droite, etc. Retirer carrés 1 et 16. Pour commencer la preuve, notez que le carré 2 est couvert soit par un domino posé horizontalement, qui recouvre ers carrés 2 et 3, ou verticalement, qui couvre les carrés 2 et 6. Examinez chacun de ces cas séparément et travaillez à travers tous les sous-cas qui se présentent.]

∗ **46.** Prouver que lorsqu'un carré blanc et un carré noir sont retiré d'un damier 8×8 (coloré comme dans le texte), vous pouvez carreler les carrés restants du planche à l'aide de dominos. [*Astuce:* montrez que lorsqu'un noir et un carré blanc sont supprimés, chaque partie de la partici- tion des cellules restantes formées en insérant les barrières montré sur la figure peut être recouvert de dominos.]

47. Montrez qu'en supprimant deux carrés blancs et deux noirs carrés d'un damier 8×8 (colorés comme dans le texte), vous pouvez rendre impossible la mosaïque du reste carrés utilisant des dominos.

∗ **48.** Trouver tous les carrés, s'ils existent, sur un damier 8×8 de telle sorte que la planche obtenue en retirant l'un de ces le carré peut être carrelé à l'aide de triominos droits. [*Indice: d'* abord utiliser des arguments basés sur la coloration et les rotations pour associer autant de carrés que possible à l'examen.]

∗ **49. a)** Dessinez chacun des cinq tétrominos différents, où un le tétromino est un polyomino composé de quatre carrés.

b) Pour chacun des cinq tétrominoes différents, prouver ou prouver que vous pouvez carreler un damier standard en utilisant ces tétrominos.

∗ **50.** Prouvez ou réfutez que vous pouvez carreler un damier 10×10 planche en utilisant des tétrominos droits.

Termes et résultats clés

TERMES

proposition: une affirmation vraie ou fausse

variable propositionnelle: variable qui représente une proposition tion

valeur de vérité: vrai ou faux

¬ *p* (négation de *p*): la proposition avec la valeur de vérité opposée à la valeur de vérité de *p*

opérateurs logiques: opérateurs utilisés pour combiner des propositions

proposition composée: une proposition construite par faire des propositions en utilisant des opérateurs logiques

table de vérité: une table affichant toutes les valeurs de vérité possibles de propositions

$p \vee q$ (disjonction de *p* et *q*): la proposition « *p* ou *q* », qui est vrai si et seulement si au moins l'un des *p* et *q* est vrai

$p \wedge q$ (conjonction de p et q): la proposition « p et q » ce qui est vrai si et seulement si p et q sont vrais

$p \oplus q$ (exclusif ou de p et q): la proposition « p *XOR* q », ce qui est vrai lorsque exactement l'un des p et q est vrai

$p \to q$ (p implique q): la proposition «si p , alors q », qui est faux si et seulement si p est vrai et q est faux

inverse de $p \to q$: l'instruction conditionnelle $q \to p$

contrapositif de $p \to q$: l'énoncé conditionnel $\neg q \to \neg p$

inverse de $p \to q$: l'instruction conditionnelle $\neg p \to \neg q$

$p \leftrightarrow q$ (biconditionnel): la proposition « p si et seulement si q », ce qui est vrai si et seulement si p et q ont la même vérité valeur

bit: soit un 0 soit un 1

Variable booléenne: une variable qui a une valeur de 0 ou 1

opération bit: une opération sur un ou plusieurs bits

chaîne de bits: une liste de bits

opérations au niveau du bit: opérations sur les chaînes de bits qui fonctionnent sur chaque bit dans une chaîne et le bit correspondant dans l'autre chaîne

porte logique: un élément logique qui effectue une opération logique sur un ou plusieurs bits pour produire un bit de sortie

circuit logique: un circuit de commutation composé de portes logiques qui produit un ou plusieurs bits de sortie

tautologie: une proposition composée toujours vraie

contradiction: une proposition composée toujours fausse

contingence: une proposition composée qui est parfois vraie et parfois faux

propositions composées cohérentes: propositions composées pour laquelle il existe une affectation de valeurs de vérité aux aptes qui rend toutes ces propositions vraies

proposition composée satisfaisable: une proposition composée pour laquelle il existe une affectation de valeurs de vérité à ses aptes qui le rendent vrai

propositions composées logiquement équivalentes: composé propositions qui ont toujours les mêmes valeurs de vérité

prédicat: partie d'une phrase qui attribue une propriété au matière

fonction propositionnelle: une déclaration contenant un ou plusieurs variables qui deviennent une proposition lorsque chacune de ses ables se voit attribuer une valeur ou est lié par un quantificateur

domaine (ou univers) du discours: les valeurs d'une variable dans un la fonction propositionnelle peut prendre

$\exists x P(x)$ (quantification existentielle de $P(x)$): la proposition c'est vrai si et seulement s'il existe un x dans le domaine tel que $P(x)$ est vrai

$\forall x P(x)$ (quantification universelle de $P(x)$): la proposition cela est vrai si et seulement si $P(x)$ est vrai pour chaque x dans le domaine

expressions logiquement équivalentes: expressions qui ont le même valeur de vérité, quelles que soient les fonctions propositionnelles et les domaines sont utilisés

variable libre: une variable non liée dans une fonction propositionnelle

variable liée: une variable qui est quantifiée

portée d'un quantificateur: partie d'une instruction où le quan-tifier lie sa variable

argument: une séquence d'instructions

forme d'argument: une séquence de propositions composées ing des variables propositionnelles

prémisse: une déclaration, sous forme d'argument, ou sous forme d'argument, autre que le dernier

conclusion: la déclaration finale dans un argument ou un argument forme

forme d'argument valide: une séquence de propositions composées impliquant des variables propositionnelles où la vérité de tous les prémisses implique la vérité de la conclusion

argument valide: un argument avec une forme d'argument valide

règle d'inférence: une forme d'argument valide qui peut être utilisée dans la démonstration que les arguments sont valides

erreur: une forme d'argument invalide souvent utilisée incorrectement comme règle d'inférence (ou parfois, plus généralement, une incorporation argument correct)

raisonnement circulaire ou mendicité: raisonnement où une ou plusieurs étapes sont basées sur la véracité de la déclaration être prouvé

théorème: une affirmation mathématique qui peut être vrai

conjecture: une affirmation mathématique proposée pour être vraie, mais cela n'a pas été prouvé

preuve: une démonstration qu'un théorème est vrai

axiome: une déclaration qui est supposée être vraie et qui peut être utilisé comme base pour prouver des théorèmes

lemme: un théorème utilisé pour prouver d'autres théorèmes

corollaire: une proposition qui peut être prouvée en conséquence d'un théorème qui vient d'être prouvé

preuve vide: une preuve que $p \to q$ est vrai basé sur le fait que p est faux

preuve triviale: une preuve que $p \to q$ est vraie basée sur le fait que q est vrai

preuve directe: une preuve que $p \to q$ est vraie qui procède en montrant que q doit être vrai lorsque p est vrai

preuve par contraposition: une preuve que $p \to q$ est vrai que ceeds en montrant que p doit être faux quand q est faux

preuve par contradiction: une preuve que p est vrai sur la base de la vérité de l'énoncé conditionnel $\neg p \to q$, où q est un contradiction

preuve exhaustive: une preuve qui établit un résultat en vérifiant une liste de tous les cas possibles

preuve par cas: une preuve divisée en cas séparés, lorsque ceux-ci les étuis couvrent toutes les possibilités

sans perte de généralité: une hypothèse dans une preuve qui fait il est possible de prouver un théorème en réduisant le nombre de cas à considérer dans la preuve

contre-exemple: un élément x tel que $P(x)$ est faux

preuve d'existence constructive: une preuve qu'un élément avec un la propriété spécifiée existe qui trouve explicitement un tel élément ment

preuve d'existence non constructive: une preuve qu'un élément avec il existe une propriété spécifiée qui ne trouve pas explicitement une telle un élément

nombre rationnel: un nombre qui peut être exprimé comme le rapport de deux entiers p et q tels que $q = 0$

preuve d'unicité: une preuve qu'il y a exactement un élément satisfaire une propriété spécifiée

RÉSULTATS

Les équivalences logiques données dans les tableaux 6, 7 et 8 de la tion 1.3.

Les lois de De Morgan pour les quantificateurs.

Règles d'inférence pour le calcul propositionnel.

Règles d'inférence pour les déclarations quantifiées.

Questions de révision

1. a) Définissez la négation d'une proposition.

b) Quelle est la négation de «Ceci est un cours ennuyeux»?

2. a) Définissez (en utilisant des tables de vérité) la disjonction, tion, exclusive ou conditionnelle et biconditionnelle de les propositions p et q .

b) Donner un exemple de prédicat $P(x, y)$ tel que $\exists x \forall y P(x, y)$ et $\forall y \exists x P(x, y)$ ont une vérité différente valeurs.

8. Décrivez ce que signifie un argument valable dans la proposition logique internationale et montrent que l'argument «Si la terre est

b) Quelles sont la disjonction, la conjonction, l'exclusivité ou, conditionnelle et biconditionnelle des propositions «Je vais aller au cinéma ce soir "et" je vais finir mon discret devoirs de mathématiques »?

3. a) Décrivez au moins cinq façons différentes d'écrire la déclaration supplémentaire $p \to q$ en anglais.

b) Définir l'inverse et contrapositif d'un conditionnel déclaration.

c) Énoncer l'inverse et la contrapositive de l'accord déclaration supplémentaire "S'il fait beau demain, alors je allez vous promener dans les bois.

4. a) Que signifie que deux propositions soient logiquement équivalent?

b) Décrivez les différentes manières de montrer que deux les propositions de livre sont logiquement équivalentes.

c) Montrer d'au moins deux manières différentes que le composé les propositions $\neg p \lor (r \to \neg q)$ et $\neg p \lor \neg q \lor \neg r$ sont équivalent.

5. *(dépend de l'ensemble d'exercices de la section 1.3)*

a) Étant donné une table de vérité, expliquez comment utiliser la nor- forme mal pour construire une proposition composée avec cette table de vérité.

b) Expliquez pourquoi la partie (a) montre que les opérateurs ∧, ∨, et ¬ sont fonctionnellement complets.

c) Existe-t-il un opérateur tel que l'ensemble contenant juste cet opérateur est fonctionnellement complet?

6. Quelles sont les quantifications universelles et existentielles de un prédicat $P(x)$? Quelles sont leurs négations?

7. a) Quelle est la différence entre la quantification $\exists x \forall y P(x, y)$ et $\forall y \exists x P(x, y)$, où $P(x, y)$ est un prédicat?

plat, alors vous pouvez naviguer au bord de la terre, "" Vous pouvez- pas naviguer du bord de la terre ", par conséquent," La terre est pas plat »est un argument valable.

9. Utilisez des règles d'inférence pour montrer que si les locaux «Tous les zèbres ont des rayures "et" Mark est un zèbre "sont vrais, alors la conclusion «Mark a des rayures» est vraie.

10. a) Décrivez ce qu'on entend par une preuve directe, une preuve par contravention, et une preuve par contradiction d'une con- instruction supplémentaire $p \to q$.

b) Donner une preuve directe, une preuve par contraposition et un preuve par contradiction de l'énoncé: «Si n est pair, alors $n + 4$ est pair. "

11. a) Décrire une façon de prouver la biconditional $p \leftrightarrow q$.

b) Démontrez l'énoncé: «L'entier $3n + 2$ est impair si et seulement si l'entier $9n + 5$ est pair, où n est un entier ger. "

12. Pour prouver que les énoncés p_1 , p_2 , p_3 et p_4 sont équivalents est-il suffisant de montrer que les déclarations conditionnelles $p_4 \to p_2$, $p_3 \to p_1$ et $p_1 \to p_2$ sont valides? Sinon, vide une autre collection de déclarations conditionnelles qui peuvent être utilisé pour montrer que les quatre déclarations sont équivalentes.

13. a) Supposons qu'une déclaration de la forme $\forall x P(x)$ soit fausse. Comment cela peut-il être prouvé?

b) Montrer que l'énoncé «Pour tout entier positif n , $n^2 \geq 2n$ "est faux.

14. Quelle est la différence entre une approche constructive et non preuve d'existence constructive? Donnez un exemple de chaque.

15. Quels sont les éléments d'une preuve de l'existence d'un élément x tel que $P(x)$, où $P(x)$ est une propositionnelle une fonction?

16. Expliquez comment une preuve par cas peut être utilisée pour prouver un résultat sur les valeurs absolues, comme le fait que $|xy| = |x||y|$ pour tous les nombres réels x et y .

Exercices supplémentaires

1. Soit p la proposition «Je ferai tous les exercices ce livre "et q soit la proposition" je vais obtenir un "A" dans ce cours. »Exprimez chacun de ces éléments sous la forme d'une p et q .

a) Je n'obtiendrai un «A» dans ce cours que si je fais tous les Cise dans ce livre.

b) Je vais obtenir un «A» dans ce cours et je ferai tout exercice dans ce livre.

c) Soit je n'obtiendrai pas de «A» dans ce cours, soit je n'obtiendrai pas faites tous les exercices de ce livre.

d) Pour obtenir un «A» dans ce cours, il est nécessaire et suffisant que je fasse tous les exercices de ce livre.

2. Trouvez la table de vérité de la proposition composée $(p \lor q) \to (p \land \neg r)$.

3. Montrer que ces propositions composées sont des tautologies.

a) $(\neg q \land (p \to q)) \to \neg p$
b) $((p \lor q) \land \neg p) \to q$

4. Donnez l'inverse, la contrapositive et l'inverse de ces déclarations conditionnelles.

a) S'il pleut aujourd'hui, je me rendrai au travail.
b) Si $|x| = x$, puis $x \geq 0$.
c) Si n est supérieur à 3, alors n^2 est supérieur à 9.

5. Étant donné un énoncé conditionnel $p \to q$, trouver l'inverse de son inverse, l'inverse de son inverse, et le con- verset de sa contrapositive.

6. Étant donné une instruction conditionnelle $p \to q$, trouver l'inverse de son inverse, l'inverse de son inverse, et l'inverse de son contrapositif.

7. Trouver une proposition composée impliquant la propositionnelle variables p , q , r et s qui est vrai lorsque exactement trois des ces variables propositionnelles sont vraies et fausses sinon sage.

8. Montrez que ces déclarations sont incohérentes: «Si Sergei accepte l'offre d'emploi, il recevra une prime de signature. "" Si Sergei accepte l'offre d'emploi, puis il recevra un salaire. "" Si Sergei reçoit une prime de signature, il ne sera pas recevoir un salaire plus élevé. "" Sergei accepte l'offre d'emploi. "

9. Montrez que ces déclarations sont incohérentes: «Si Miranda ne suit pas de cours de mathématiques discrètes, alors elle

13. Supposons que vous rencontriez trois personnes Aaron, Bohan et Cristal. Pouvez-vous déterminer ce que Aaron, Bohan et Crys- sont si Aaron dit "Nous sommes tous des fripons" et Bohan dit "Exactement l'un d'entre nous est un coquin."?

14. Supposons que vous rencontriez trois personnes, Anita, Boris et Carmen. Que sont Anita, Boris et Carmen si Anita dit "Je suis un mec et Boris est un chevalier" et Boris dit "Ex- en fait l'un de nous trois est chevalier »?

15. (Adapté de [Sm78]) Supposons que sur une île il sont trois types de personnes, chevaliers, cavaliers et normaux (également connu sous le nom d'espions). Les chevaliers disent toujours la vérité, les fripons mentent toujours, et les normales mentent parfois et les fois disent la vérité. Les détectives ont interrogé trois habitants tants de l'île - Amy, Brenda et Claire - dans le cadre de l'enquête sur un crime. Les détectives savaient que l'un des trois a commis le crime, mais pas lequel. Ils savaient également que le criminel était un chevalier et que les deux autres ne l'étaient pas. De plus, les détectives ont enregistré ces déclarations: Amy: «Je suis innocente». Brenda: «Que Amy dit que c'est vrai. "Claire:" Brenda n'est pas une normale. "Af- après avoir analysé leurs informations, les détectives ont identifié le coupable. Qui était-ce?

16. Montrer que si S est une proposition, où S est le conditionnel «Si S est vrai, alors les licornes vivent», puis «Uni- cors vivent »est vrai. Montrer qu'il s'ensuit que S ne peut pas être un proposition. (Ce paradoxe est connu comme *le paradoxe de Löb* .)

17. Montrer que l'argument avec les prémisses «La fée des dents est un vraie personne "et" La fée des dents n'est pas une vraie personne "et ne sera pas diplômé. "" Si Miranda n'obtient pas son diplôme, alors elle n'est pas qualifiée pour le poste. »« Si Miranda lit ceci livre, puis elle est qualifiée pour le travail. "" Miranda ne pas suivre un cours de mathématiques discrètes mais elle lit ce livre."

Les enseignants du Moyen Âge auraient testé le temps réel capacité logique propositionnelle d'un élève via une technique connue comme un **jeu obligato** . Dans un jeu obligato, plusieurs tours est fixé et à chaque tour, l'enseignant donne à l'étudiant la affirmations affirmatives selon lesquelles l'étudiant doit accepter ou rejeter ils sont donnés. Lorsque l'élève accepte une affirmation, il est ajouté comme engagement; lorsque l'étudiant rejette une affirmation sa négation est ajoutée comme un engagement. L'étudiant passe le test si la cohérence de tous les engagements est maintenue tout au long du test.

10. Supposons que dans un jeu obligato à trois tours, l'enseignant donne d'abord à l'étudiant la proposition $p \rightarrow q$, puis proposition $\neg (p \vee r) \vee q$, et enfin la proposition q . Pour laquelle des huit séquences possibles de trois réponses l'élève réussira-t-il le test?

11. Supposons que dans un jeu obligato à quatre tours, l'enseignant donne d'abord à l'étudiant la proposition $\neg (p \rightarrow (q \wedge r))$, puis la proposition $p \vee \neg q$, puis la proposition $\neg r$, et enfin, la proposition $(p \wedge r) \vee (q \rightarrow p)$. Pour lequel de les 16 séquences possibles de quatre réponses seront l'étudiant passer le test?

12. Expliquez pourquoi chaque jeu obligato a une stratégie gagnante.

Les exercices 13 et 14 se déroulent sur l'île des chevaliers et des nègres décrit dans l'exemple 7 de la section 1.2.

conclusion "Vous pouvez trouver de l'or au bout de l'arc-en-ciel" est un argument valide. Cela montre-t-il que la conclusion est vrai?

18. Supposons que la valeur de vérité de la proposition p_i soit **T** chaque fois que i est un entier positif impair et est **F** quand-jamais i est un entier encore positif. Trouvez les valeurs de vérité de $\bigvee_{i=1}^{100} (p_i \wedge p_{i+1})$ et $\bigwedge_{i=1}^{100} (p_i \vee p_{i+1})$.

∗ **19.** Puzzles Sudoku 16 × 16 (avec blocs 4 × 4) comme problèmes de satisfiabilité.

20. Soit $P(x)$ l'énoncé «L'élève x connaît le calcul» et soit $Q(y)$ l'énoncé «La classe y contient un élève qui connaît le calcul. »Exprimez chacun de ces éléments sous forme de quantifications de $P(x)$ et $Q(y)$.

a) Certains élèves connaissent le calcul.

b) Tous les élèves ne connaissent pas le calcul.

c) Chaque classe a un élève qui connaît le calcul.

d) Chaque élève de chaque classe connaît le calcul.

e) Il y a au moins une classe sans élève qui sait calcul.

21. Soit $P(m, n)$ l'énoncé « m divise n », où le domain pour les deux variables se compose de tous les entiers positifs. (Par « m divise n », nous voulons dire que $n = km$ pour un entier k .) Déterminez les valeurs de vérité de chacune de ces déclarations.

a) $P(4, 5)$ **b)** $P(2, 4)$
c) $\forall m \forall n P(m, n)$ **d)** $\exists m \forall n P(m, n)$
e) $\exists n \forall m P(m, n)$ **f)** $\forall n P(1, n)$

22. Trouver un domaine pour les quantificateurs dans $\exists x \exists y (x = y \wedge \forall z ((z = x) \vee (z = y)))$ telle que cette affirmation est vraie.

23. Trouver un domaine pour les quantificateurs dans $\exists x \exists y (x = y \wedge \forall z ((z = x) \vee (z = y)))$ de sorte que cette affirmation est fausse.

24. Utilisez des quantificateurs existentiels et universels pour exprimer déclaration «Personne n'a plus de trois grands-mères» la fonction propositionnelle $G(x, y)$, qui représente " X est la grand-mère de y ."

25. Utilisez des quantificateurs existentiels et universels pour exprimer déclaration "Tout le monde a exactement deux parents biologiques" utilisant la fonction propositionnelle $P(x, y)$, qui représente envoie « x est le parent biologique de y ».

26. Le quantificateur $\exists_n$ désigne «il existe exactement n », de sorte que $\exists_n x P(x)$ signifie qu'il existe exactement n valeurs dans le do-principal tel que $P(x)$ soit vrai. Déterminer la vraie valeur de ces déclarations où le domaine se compose de tous réels Nombres.

a) $\exists_0 x (x^2 = -1)$ **b)** $\exists_1 x (|x| = 0)$
c) $\exists_2 x (x^2 = 2)$ **d)** $\exists_3 x (x = |x|)$

27. Exprimez chacune de ces déclarations en utilisant des quantificateurs universels et logique propositionnelle où $\exists_n$ est défini dans l'exercice 26.

a) $\exists_0 x P(x)$ **b)** $\exists_1 x P(x)$
c) $\exists_2 x P(x)$ **d)** $\exists_3 x P(x)$

28. Soit $P(x, y)$ une fonction propositionnelle. Montre CA $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$ est une tautologie.

29. Soit $P(x)$ et $Q(x)$ des fonctions propositionnelles. Spectacle que $\exists x (P(x) \rightarrow Q(x))$ et $\forall x P(x) \rightarrow \exists x Q(x)$ toujours ont la même valeur de vérité.

30. Si $\forall y \exists x P(x, y)$ est vrai, cela signifie-t-il nécessairement que $\exists x \forall y P(x, y)$ est vrai?

31. Si $\forall x \exists y P(x, y)$ est vrai, cela signifie-t-il nécessairement que $\exists x \forall y P(x, y)$ est vrai?

32. Trouvez les négations de ces déclarations.

a) S'il neige aujourd'hui, j'irai skier demain.

b) Chaque personne de cette classe comprend les mathématiques induction.

c) Certains élèves de cette classe n'aiment pas les mathématiques discrètes ématiques.

d) Dans chaque classe de mathématiques, il y a un élève qui s'endort pendant les cours.

33. Exprimez cette affirmation en utilisant des quantificateurs: «Chaque élève dans cette classe a pris un cours dans chaque département à l'école des sciences mathématiques. "

34. Exprimez cette affirmation à l'aide de quantificateurs: «Il existe un sur le campus de certains collèges aux États-Unis en dont chaque pièce est peinte en blanc.

35. Exprimez la déclaration «Il y a exactement un étudiant dans ce classe qui a pris exactement une classe de mathématiques à ce l'école »en utilisant le quantificateur d'unicité. Alors exprime ça instruction utilisant des quantificateurs, sans utiliser l'unicité quantificateur.

36. Décrivez une règle d'inférence qui peut être utilisée pour prouver que il y a exactement deux éléments x et y dans un domaine tel que $P(x)$ et $P(y)$ sont vrais. Exprimer cette règle d'inférence comme une déclaration en anglais.

37. Utiliser des règles d'inférence pour montrer que si les locaux $\forall x (P(x) \rightarrow Q(x))$, $\forall x (Q(x) \rightarrow R(x))$ et $\neg R(a)$, où a est dans le domaine, sont vrais, alors la conclusion $\neg P(a)$ est vrai.

38. Montrer que si x^3 est irrationnel, alors x est irrationnel.

39. Montrer que si x est irrationnel et $x \geq 0$, alors $\sqrt{x}$ est irrationnel.

40. Démontrer qu'étant donné un entier non négatif n , il existe un entier non négatif m tel que $m^2 \leq n < (m + 1)^2$.

41. Démontrer qu'il existe un entier m tel que $m^2 > 10^{1000}$. Votre preuve est-elle constructive ou non constructive?

42. Démontrer qu'il existe un entier positif qui peut être écrit comme la somme des carrés d'entiers positifs dans deux diffé-différentes manières. (Utilisez un ordinateur ou une calculatrice pour accélérer votre travail.)

43. réfuter la déclaration selon laquelle chaque entier positif est le somme des cubes de huit entiers non négatifs.

44. réfuter l'affirmation selon laquelle chaque entier positif est le somme d'au plus deux carrés et un cube non négatif entiers.

45. réfuter l'affirmation selon laquelle chaque entier positif est le somme de 36 cinquièmes puissances d'entiers non négatifs.

46. En supposant la vérité du théorème qui dit que $\sqrt{n}$ est irrationnel chaque fois que n est un entier positif qui n'est pas un carré parfait, prouve que $\sqrt{2} + \sqrt{3}$ est irrationnel.

Projets informatiques

Écrivez des programmes avec l'entrée et la sortie spécifiées.

1. Étant donné les valeurs de vérité des propositions p et q , trouver le les valeurs de vérité de la conjonction, de la disjonction, de l'exclusivité ou, conditionnelle et biconditionnelle de ces propositions. tions.

2. Étant donné deux chaînes de bits de longueur n , trouvez le *ET au niveau* du bit , *OR au niveau du* bit et *XOR au niveau* du bit de ces chaînes.

∗ **3.** Donnez une proposition composée, déterminez si elle est en vérifiant sa valeur de vérité pour toutes les affectations positives. des valeurs de vérité à ses variables propositionnelles.

4. Étant donné les valeurs de vérité des propositions p et q dans la logique floue, trouver la valeur de vérité de la disjonction et la conjonction de p et q (voir les exercices 46 et 47 de Section 1.1).

∗ **5.** Étant donné les entiers positifs m et n , jouez au jeu de manière interactive de Chomp.

∗ **6.** Étant donné une partie d'un damier, recherchez les pavages de ce damier avec différents types de polyominos, y compris dominos, les deux types de triominos et les plus grands polyomi- non.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Recherchez des entiers positifs qui ne sont pas la somme des cubes de neuf entiers positifs différents.

2. Recherchez les entiers positifs supérieurs à 79 qui ne sont pas les somme des quatrièmes puissances de 18 entiers positifs.

3. Trouvez autant d'entiers positifs que possible qui peuvent être écrits dix comme la somme des cubes d'entiers positifs, dans deux différents façons, partageant cette propriété avec 1729.

∗ **4.** Essayez de trouver des stratégies gagnantes pour le jeu de Chomp pour différentes configurations initiales de cookies.

5. Construisez les 12 pentominos différents, où un pentomino est un polyomino composé de cinq carrés.

6. Trouvez tous les rectangles de 60 carrés qui peuvent être carrelés en utilisant chacun des 12 pentominos différents.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Discutez des paradoxes logiques, y compris le paradoxe de menides le Crétois, le paradoxe de la carte de Jourdain, et le bar- le paradoxe des ber, et comment ils sont résolus.

2. Décrire comment la logique floue est appliquée aux applications pratiques plications. Consultez un ou plusieurs des livres récents sur logique floue écrite pour un public général.

3. Décrivez certains des problèmes pratiques qui peuvent être considérés comme des problèmes de satisfiabilité.

4. Décrivez certaines des techniques qui ont été conçues pour aider les gens à résoudre des puzzles de Sudoku sans utiliser de ordinateur.

5. Décrivez les règles de base de *WFF'N PROOF* , *The Game of Modern Logic* , développé par Layman Allen. Donner un examen ples de certains des jeux inclus dans *WFF'N PROOF* .

6. Lisez certains des écrits de Lewis Carroll sur symbolique logique. Décrivez en détail certains des modèles qu'il utilisait représenter des arguments logiques et les règles d'inférence qu'il utilisé dans ces arguments.

7. Étendre la discussion sur Prolog donnée dans la section 1.4, ex- expliquant plus en détail comment Prolog utilise la résolution.

8. Discutez de certaines des techniques utilisées en informatique logique, y compris la règle de Skolem.

9. **La** «démonstration automatisée des théorèmes» consiste à utiliser des puters pour prouver mécaniquement les théorèmes. Discutez des objectifs et applications de la démonstration automatisée de théorèmes et progrès réalisés dans le développement de prouveurs de théorèmes automatisés.

10. Décrire comment le calcul de l'ADN a été utilisé pour résoudre exemples du problème de satisfiabilité.

11. Recherchez certaines des preuves incorrectes de la célèbre ouverture questions et questions ouvertes résolues depuis 1970 et décrire le type d'erreur commise dans chaque preuve.

12. Discutez de ce que l'on sait des stratégies gagnantes dans le jeu de Chomp.

13. Décrivez divers aspects de la stratégie de preuve examinés par George Pólya dans ses écrits sur le raisonnement, y compris [Po62], [Po71] et [Po90].

14. Décrivez quelques problèmes et résultats concernant les pavages polyominos, comme décrit dans [Go94] et [Ma91], par exemple ample.

CHAPITRE

Structures de base: ensembles, fonctions, Séquences, sommes et matrices

Une grande partie des mathématiques discrètes est consacrée à l'étude des structures discrètes, envoyé des objets discrets. De nombreuses structures discrètes importantes sont construites à l'aide d'ensembles, qui sont collections d'objets. Parmi les structures discrètes construites à partir d'ensembles figurent des combinaisons, non ordonnées collections d'objets largement utilisés pour le comptage; relations, ensembles de paires ordonnées qui représentent relations entre objets; graphiques, ensembles de sommets et d'arêtes qui relient les sommets; et fini machines d'état, utilisées pour modéliser des machines informatiques. Ce sont quelques-uns des sujets que nous étudierons dans les chapitres suivants.

Le concept d'une fonction est extrêmement important en mathématiques discrètes. Une fonction attribue à chaque élément d'un premier ensemble exactement un élément d'un deuxième ensemble, où les deux ensembles ne sont pas nécessairement distinct. Les fonctions jouent un rôle important dans les mathématiques discrètes. Elles sont utilisé pour représenter la complexité de calcul des algorithmes, pour étudier la taille des ensembles, pour compter objets, et dans une myriade d'autres façons. Les structures utiles telles que les séquences et les chaînes sont types spéciaux de fonctions. Dans ce chapitre, nous introduirons la notion de séquence, qui représente des listes ordonnées d'éléments. En outre, nous présenterons certains types importants de séquences et nous montrerons comment définir les termes d'une séquence en utilisant des termes antérieurs. Nous allons abordent également le problème de l'identification d'une séquence à partir de ses premiers termes.

Dans notre étude des mathématiques discrètes, nous ajouterons souvent des termes consécutifs d'une séquence de Nombres. Parce que l'ajout de termes à partir d'une séquence, ainsi que d'autres ensembles de nombres indexés, est une telle occurrence commune, une notation spéciale a été développée pour ajouter de tels termes. Dans ce chapitre, nous introduirons la notation utilisée pour exprimer les sommations. Nous développerons des formules pour certains types de sommations qui apparaissent tout au long de l'étude des mathématiques discrètes. Pour Par exemple, nous rencontrerons ces sommations dans l'analyse du nombre d'étapes utilisées par un algorithme pour trier une liste de nombres afin que ses termes soient en ordre croissant.

Les tailles relatives des ensembles infinis peuvent être étudiées en introduisant la notion de taille, ou cardinalité, d'un ensemble. On dit qu'un ensemble est dénombrable quand il est fini ou a la même taille que le ensemble d'entiers positifs. Dans ce chapitre, nous établirons le résultat surprenant que l'ensemble des les nombres rationnels sont dénombrables, tandis que l'ensemble des nombres réels ne l'est pas. Nous montrerons également comment les concepts dont nous discutons peuvent être utilisés pour montrer qu'il existe des fonctions qui ne peuvent pas être calculées en utilisant un programme informatique dans n'importe quel langage de programmation.

Les matrices sont utilisées en mathématiques discrètes pour représenter une variété de structures discrètes. nous examinera le matériel de base sur les matrices et l'arithmétique des matrices nécessaires pour représenter les relations et graphiques. L'arithmétique matricielle que nous étudions sera utilisée pour résoudre une variété de problèmes impliquant ces structures.

Ensembles

introduction

Dans cette section, nous étudions la structure discrète fondamentale sur laquelle toutes les autres structures discrètes sont construits, à savoir, l'ensemble. Les ensembles sont utilisés pour regrouper des objets. Souvent, mais pas toujours, les objets d'un ensemble ont des propriétés similaires. Par exemple, tous les étudiants actuellement inscrits dans votre école, composez un ensemble. De même, tous les étudiants qui suivent actuellement un cours en les mathématiques de n'importe quelle école constituent un ensemble. De plus, les élèves inscrits dans votre école qui suivent un cours de mathématiques discrètes forment un ensemble qui peut être obtenu en prenant le éléments communs aux deux premières collections. Le langage des ensembles est un moyen d'étudier collections de façon organisée. Nous fournissons maintenant une définition d'un ensemble. Cette définition est un définition intuitive, qui ne fait pas partie d'une théorie formelle des ensembles.

DÉFINITION 1 Un *ensemble* est une collection non ordonnée d'objets, appelés *éléments* ou *membres* de l'ensemble. Un ensemble est dit *contenir* ses éléments. On écrit *un* $\in A$ pour indiquer que *un* est un élément de l'ensemble A . le notation d' *un* $\in A$ indique que *la* constitue pas un élément de l'ensemble A .

Il est courant que les ensembles soient indiqués en lettres majuscules. Les lettres minuscules sont généralement utilisé pour désigner des éléments d'ensembles.

Il existe plusieurs façons de décrire un ensemble. Une façon consiste à répertorier tous les membres d'un ensemble, lorsque c'est possible. Nous utilisons une notation où tous les membres de l'ensemble sont répertoriés entre accolades. Pour par exemple, la notation $\{a, b, c, d\}$ représente l'ensemble avec les quatre éléments a, b, c et d . Cette La manière de décrire un ensemble est connue sous le nom de **méthode de liste** .

EXEMPLE 1 L'ensemble V de toutes les voyelles de l'alphabet anglais peut s'écrire $V = \{a, e, i, o, u\}$. ▲

EXEMPLE 2 L'ensemble O d'entiers positifs impairs inférieurs à 10 peut être exprimé par $O = \{1, 3, 5, 7, 9\}$. ▲

EXEMPLE 3 Bien que les ensembles soient généralement utilisés pour regrouper des éléments ayant des propriétés communes, il existe rien qui n'empêche un ensemble d'avoir des éléments apparemment sans rapport. Par exemple, $\{a, 2,$ Fred, New Jersey$\}$ est l'ensemble contenant les quatre éléments a , 2, Fred et New Jersey. ▲

Parfois, la méthode de la liste est utilisée pour décrire un ensemble sans répertorier tous ses membres. Certains les membres de l'ensemble sont répertoriés, puis des *ellipses* (...) sont utilisées lorsque le motif général du éléments est évident.

EXEMPLE 4 L'ensemble des entiers positifs inférieurs à 100 peut être noté $\{1, 2, 3, ..., 99\}$. ▲

Une autre façon de décrire un ensemble consiste à utiliser **la** notation de **générateur d'ensemble** . Nous caractérisons tous ceux éléments de l'ensemble en indiquant la ou les propriétés dont ils doivent être membres Pour par exemple, l'ensemble O de tous les entiers positifs impairs inférieurs à 10 peut être écrit comme

$O = \{x \mid x$ est un entier positif impair inférieur à $10\}$,

ou, en spécifiant l'univers comme l'ensemble des entiers positifs, comme

$O = \{x \in \mathbf{Z}^+ \mid x$ est impair et $x < 10\}$.

Nous utilisons souvent ce type de notation pour décrire les ensembles lorsqu'il est impossible de lister tous les éléments de l'ensemble. Par exemple, l'ensemble $\mathbf{Q}^+$ de tous les nombres rationnels positifs peuvent s'écrire

$\mathbf{Q}^+ = \{x \in \mathbf{R} \mid x = \frac{p}{q}$, pour certains entiers positifs p et $q\}$.

Attention à cette maturité les maticiens sont en désaccord si 0 est naturel nombre. Nous le considérons tout à fait naturel.

Ces ensembles, chacun désigné par une lettre en gras, jouent un rôle important dans les mathématiques discrètes. matiques:

$\mathbf{N} = \{0, 1, 2, 3, ...\}$, l'ensemble des **nombres naturels**
$\mathbf{Z} = \{..., -2, -1, 0, 1, 2, ...\}$, l'ensemble des **entiers**
$\mathbf{Z}^+ = \{1, 2, 3, ...\}$, l'ensemble des **entiers positifs**
$\mathbf{Q} = \{p/q \mid p \in \mathbf{Z}, q \in \mathbf{Z}$, et $q = 0\}$, l'ensemble des **nombres rationnels**
$\mathbf{R}$, l'ensemble des **nombres réels**
$\mathbf{R}^+$, l'ensemble des **nombres réels positifs**
$\mathbf{C}$, l'ensemble des **nombres complexes** .

(Notez que certaines personnes ne considèrent pas 0 comme un nombre naturel, alors faites attention à vérifier comment le terme *les nombres naturels* sont utilisés lorsque vous lisez d'autres livres.)

Rappelez la notation des **intervalles** de nombres réels. Quand a et b sont des nombres réels avec $a < b$, on écrit

$$[a, b] = \{x \mid a \leq x \leq b\}$$

$$[a, b) = \{x \mid a \leq x < b\}$$

$$(a, b] = \{x \mid a < x \leq b\}$$

$$(a, b) = \{x \mid a < x < b\}$$

Notez que $[a, b]$ est appelé l'**intervalle fermé** de a à b et (a, b) est appelé l'**intervalle ouvert** de a à b.

Les ensembles peuvent avoir d'autres ensembles en tant que membres, comme l'illustre l'exemple 5.

EXEMPLE 5 L'ensemble $\{\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}\}$ est un ensemble contenant quatre éléments, chacun étant un ensemble. Les quatre éléments de cet ensemble sont $\mathbf{N}$, l'ensemble des nombres naturels; $\mathbf{Z}$, l'ensemble des entiers; $\mathbf{Q}$, l'ensemble des nombres rationnels; et $\mathbf{R}$, l'ensemble des nombres réels. ▲

Remarque: Notez que le concept d'un type de données, ou type, en informatique est construit sur la concept d'un ensemble. En particulier, un **type** ou **type de données** est le nom d'un ensemble, avec un ensemble de opérations pouvant être effectuées sur des objets de cet ensemble. Par exemple, *booléen* est le nom de l'ensemble $\{0, 1\}$ avec les opérateurs sur un ou plusieurs éléments de cet ensemble, tels que AND, OR, et pas.

Parce que de nombreuses déclarations mathématiques affirment que deux collections de les objets sont vraiment le même ensemble, nous devons comprendre ce que signifie que deux ensembles sont égaux.

DÉFINITION 2 Deux ensembles sont *égaux* si et seulement s'ils ont les mêmes éléments. Par conséquent, si A et B sont des ensembles, alors A et B sont égaux si et seulement si $\forall x\,(x \in A \leftrightarrow x \in B)$. On écrit $A = B$ si A et B sont ensembles égaux.

EXEMPLE 6 Les ensembles $\{1, 3, 5\}$ et $\{3, 5, 1\}$ sont égaux, car ils ont les mêmes éléments. Notez que le l'ordre dans lequel les éléments d'un ensemble sont répertoriés n'a pas d'importance. Notez également que cela n'a pas d'importance si un élément d'un ensemble est répertorié plusieurs fois, donc $\{1, 3, 3, 3, 5, 5, 5, 5\}$ est le même que l'ensemble $\{1, 3, 5\}$ car ils ont les mêmes éléments. ▲

GEORG CANTOR (1845-1918) Georg Cantor est né à Saint-Pétersbourg, en Russie, où son père était marchand prospère. Cantor a développé son intérêt pour les mathématiques à l'adolescence. Il a commencé ses études universitaires à Zurich en 1862, mais quand son père est mort, il a quitté Zurich. Il a poursuivi ses études universitaires à l'Université de Berlin en 1863, où il a étudié auprès des éminents mathématiciens Weierstrass, Kummer et Kronecker. Il obtient son doctorat en 1867, après avoir rédigé un mémoire sur la théorie des nombres. Cantor a assumé un poste à l'Université de Halle en 1869, où il a continué à travailler jusqu'à sa mort.

Cantor est considéré comme le fondateur de la théorie des ensembles. Ses contributions dans ce domaine comprennent la découverte que le ensemble de nombres réels est indénombrable. Il est également connu pour ses nombreuses contributions importantes à l'analyse. Chantre s'intéresse également à la philosophie et écrit des articles concernant sa théorie des ensembles avec la métaphysique.

Cantor s'est marié en 1874 et a eu cinq enfants. Son tempérament mélancolique était contrebalancé par l'heureuse disposition de sa femme. Bien qu'il ait reçu un important héritage de son père, il était mal payé en tant que professeur. Pour atténuer cela, il a essayé d'obtenir un poste mieux rémunéré à l'Université de Berlin. Sa nomination a été bloquée par Kronecker, qui n'était pas d'accord avec Cantor points de vue sur la théorie des ensembles. Cantor a souffert d'une maladie mentale au cours des dernières années de sa vie. Il est décédé en 1918 d'une crise cardiaque.

LE SET VIDE Il y a un set spécial qui ne contient aucun élément. Cet ensemble est appelé l' **ensemble vide** , ou un **ensemble nul** , et est désigné par ∅. L'ensemble vide peut également être désigné par { } (c'est-à-dire que nous représentons l'ensemble vide avec une paire d'accolades qui renferme tous les éléments de cet ensemble). Souvent, un ensemble de les éléments ayant certaines propriétés se révèlent être l'ensemble nul. Par exemple, l'ensemble de tous les positifs les entiers supérieurs à leurs carrés constituent l'ensemble nul.

{∅} en a un de plus élément que ∅.

Un ensemble avec un élément est appelé un **ensemble singleton** . Une erreur courante consiste à confondre le vide définir ∅ avec l'ensemble {∅}, qui est un ensemble singleton. L'élément unique de l'ensemble {∅} est l'ensemble vide lui-même! Une analogie utile pour se souvenir de cette différence est de penser aux dossiers dans un fichier informatique système. L'ensemble vide peut être considéré comme un dossier vide et l'ensemble composé uniquement l'ensemble vide peut être considéré comme un dossier contenant exactement un dossier à l'intérieur, à savoir le dossier vide.

NAIVE SET THEORY Notez que le terme *objet* a été utilisé dans la définition d'un ensemble, Définition 1, sans préciser ce qu'est un objet. Cette description d'un ensemble en tant que collection d'objets, basé sur la notion intuitive d'un objet, a été déclaré pour la première fois en 1895 par le mathématicien Georg Cantor. La théorie qui résulte de cette définition intuitive d'un ensemble, et l'utilisation de la notion intuitive que pour toute propriété, il existe un ensemble composé exactement les objets avec cette propriété, conduisent à des **paradoxes** , ou des incohérences logiques. Cela a été montré par le philosophe anglais Bertrand Russell en 1902 (voir l'exercice 46 pour une description de l'un des ces paradoxes). Ces incohérences logiques peuvent être évitées en construisant un début de théorie des ensembles avec des axiomes. Cependant, nous utiliserons la version originale de Cantor de la théorie des ensembles, connue sous le nom de **ensemble naïf théorie** , dans ce livre parce que tous les ensembles considérés dans ce livre peuvent être traités de manière cohérente en utilisant Théorie originale de Cantor. Les élèves trouveront la familiarité avec la théorie des ensembles naïve utile s'ils continuent pour en savoir plus sur la théorie des ensembles axiomatiques. Ils découvriront également le développement de la théorie des ensembles axiomatiques beaucoup plus abstrait que le contenu de ce texte. Nous renvoyons le lecteur intéressé à [Su72] à en savoir plus sur la théorie des ensembles axiomatiques.

Diagrammes de Venn

Les ensembles peuvent être représentés graphiquement à l'aide de diagrammes de Venn, nommés d'après le cian John Venn, qui a introduit leur utilisation en 1881. Dans les diagrammes de Venn l'**ensemble universel** *U,* qui contient tous les objets considérés, est représenté par un rectangle. (Notez que l'uni-
l'ensemble versal varie en fonction des objets qui vous intéressent.) À l'intérieur de ce rectangle, des cercles ou d'autres figures géométriques sont utilisées pour représenter des ensembles. Parfois, les points sont utilisés pour représenter éléments particuliers de l'ensemble. Les diagrammes de Venn sont souvent utilisés pour indiquer les relations entre ensembles. Nous montrons comment un diagramme de Venn peut être utilisé dans l'exemple 7.

EXEMPLE 7 Dessinez un diagramme de Venn qui représente *V,* l'ensemble des voyelles de l'alphabet anglais.

Solution: Nous dessinons un rectangle pour indiquer l'ensemble universel *U* , qui est l'ensemble des 26 lettres de l'alphabet anglais. A l' intérieur de ce rectangle nous tracer un cercle pour représenter *V* . À l'intérieur de ce cercle nous indiquons les éléments de *V* avec des points (voir figure 1). ▲

U
une
u e
V
o je

FIGURE 1 **Diagramme de Venn pour l'ensemble de voyelles.**

Page 140

Sous-ensembles

Il est courant de rencontrer des situations où les éléments d'un ensemble sont également les éléments de un deuxième set. Nous introduisons maintenant une terminologie et une notation pour exprimer de telles relations entre les séries.

DÉFINITION 3 L'ensemble *A* est un *sous - ensemble* de *B* si et seulement si tous les éléments de *A* est aussi un élément de *B* . Nous utilisons la notation $A \subseteq B$ pour indiquer que *A* est un sous -ensemble de l'ensemble *B* .

On voit que $A \subseteq B$ si et seulement si la quantification

$$\forall x\,(x \in A \rightarrow x \in B)$$

est vrai. Notez que pour montrer que A n'est pas un sous-ensemble de B, il suffit de trouver un élément $x \in A$ avec $x / \in B$. Un tel x est un contre -exempleà l'affirmation selon laquelle $x \in A$ implique $x \in B$.

Nous avons ces règles utiles pour déterminer si un ensemble est un sous-ensemble d'un autre:

Montrer que A est un sous-ensemble de B Pour montrer que $A \subseteq B$, montrer que si x appartient à A alors x appartient aussi à B .

Montrer que A n'est pas un sous-ensemble de B Pour montrer que $A \subseteq B$, trouver un seul $x \in A$ tel que $x \in B$.

EXEMPLE 8 L'ensemble de tous les entiers positifs impairs inférieurs à 10 est un sous-ensemble de l'ensemble de tous les entiers positifs moins de 10, l'ensemble des nombres rationnels est un sous-ensemble de l'ensemble des nombres réels, l'ensemble de tous les ordinateurs les majors scientifiques de votre école sont un sous-ensemble de l'ensemble de tous les élèves de votre école, et l'ensemble des toutes les personnes en Chine sont un sous-ensemble de l'ensemble de toutes les personnes en Chine (c'est-à-dire que c'est un sous-ensemble de lui-même). Chacun de ces faits suit immédiatement en notant qu'un élément qui appartient au premier ensemble dans chaque paire d'ensembles appartient également au deuxième ensemble de cette paire. ▲

EXEMPLE 9 L'ensemble des entiers avec des carrés inférieurs à 100 n'est pas un sous-ensemble de l'ensemble des entiers non négatifs parce que −1 est dans l'ancien ensemble [comme $(-1)^2 < 100$], mais pas dans le dernier. L'ensemble des personnes qui avoir pris des mathématiques discrètes à votre école n'est pas un sous-ensemble de l'ensemble de l'informatique majors à votre école s'il y a au moins un élève qui a pris des mathématiques discrètes qui est pas une majeure en informatique. ▲

BERTRAND RUSSELL (1872–1970) Bertrand Russell est né dans une importante famille anglaise active dans le mouvement progressiste et ayant un fort engagement pour la liberté. Il est devenu orphelin à un âge précoce et a été confié aux parents de son père, qui l'ont fait instruire à la maison. Il est entré au Trinity College, Cambridge, en 1890, où il excellait en mathématiques et en sciences morales. Il a remporté une bourse sur la base de ses travaux sur les fondements de la géométrie. En 1910, Trinity College l'a nommé à un poste de professeur de logique et la philosophie des mathématiques.

Russell s'est battu pour des causes progressistes tout au long de sa vie. Il avait de fortes opinions pacifistes et ses protestations contre la Première Guerre mondiale a conduit à la révocation de son poste au Trinity College. Il a été emprisonné pendant 6 mois à 1918 à cause d'un article qu'il a écrit et qualifié de séditieux. Russell s'est battu pour le suffrage féminin à Great La Grande-Bretagne. En 1961, à l'âge de 89 ans, il a été emprisonné pour la deuxième fois pour ses protestations prônant le désarmement nucléaire.

Le plus grand travail de Russell était dans son développement de principes qui pourraient être utilisés comme base pour toutes les mathématiques. Le sien l'œuvre la plus célèbre est *Principia Mathematica,* écrite avec Alfred North Whitehead, qui tente de déduire toutes les mathématiques en utilisant un ensemble d'axiomes primitifs. Il a écrit de nombreux livres sur la philosophie, la physique et ses idées politiques. Russell a remporté le prix Nobel pour la littérature en 1950.

U

UNE *B*

FIGURE 2 **Diagramme de Venn Montrer que *A* est une partie de *B* .**

Le théorème 1 montre que chaque ensemble non vide S est garanti d'avoir au moins deux sous-ensembles, le ensemble vide et l'ensemble S lui - même, qui est, $\emptyset \subseteq S$ et $S \subseteq S$.

THÉORÈME 1 Pour chaque série S , (i) $\emptyset \subseteq S$ et (ii) $S \subseteq S$.

Preuve: Nous prouverons (i) et laisserons la preuve de (ii) comme exercice.

Soit S un ensemble. Pour montrer que $\emptyset \subseteq S$, nous devons montrer que $\forall x\,(x \in \emptyset \rightarrow x \in S)$ est vrai. Car l'ensemble vide ne contient aucun élément, il s'ensuit que $x \in \emptyset$ est toujours faux. Il s'ensuit que le l'énoncé conditionnel $x \in \emptyset \rightarrow x \in S$ est toujours vrai, car son hypothèse est toujours fausse et une déclaration conditionnelle avec une fausse hypothèse est vraie. Par conséquent, $\forall x\,(x \in \emptyset \rightarrow x \in S)$ est vrai. Ceci complète la preuve de (i). Notez qu'il s'agit d'un exemple de preuve vide.

Lorsque nous souhaitons souligner qu'un ensemble A est un sous-ensemble d'un ensemble B mais que $A \neq B$, nous écrivons $A \subset B$ et disons que A est un **sous - ensemble propre** de B. Pour que $A \subset B$ soit vrai, il faut que $A \subseteq B$ et il doit exister un élément x de B qui ne sont pas un élément de A . Autrement dit, A est un bon sous-ensemble de B si et seulement si

$$\forall x\,(x \in A \to x \in B) \wedge \exists x\,(x \in B \wedge x \notin A)$$

est vrai. Diagrammes de Venn peuvent être utilisés pour illustrer qu'un ensemble A est un sous -ensemble d'un ensemble B. Nous tirons la ensemble universel U en rectangle. Dans ce rectangle, nous dessinons un cercle pour B. Parce que A est un sous-ensemble de B, nous dessinons le cercle de A dans le cercle de B. Cette relation est illustrée à la figure 2.

Un moyen utile de montrer que deux ensembles ont les mêmes éléments est de montrer que chaque ensemble est un sous-ensemble de l'autre. En d'autres termes, nous pouvons montrer que si A et B sont des ensembles avec $A \subseteq B$ et $B \subseteq A$, alors $A = B$. Autrement dit, $A = B$ si et seulement si $\forall x\,(x \in A \to x \in B)$ et $\forall x\,(x \in B \to x \in A)$ ou de manière équivalente si et seulement si $\forall x\,(x \in A \leftrightarrow x \in B)$, ce qui signifie que A et B soient égal. Parce que cette méthode de montrer deux ensembles égaux est si utile, nous la mettons en évidence ici.

JOHN VENN (1834-1923) John Venn est né dans une famille de banlieue de Londres réputée pour sa philanthropie. Il a fréquenté les écoles de Londres et obtenu son diplôme de mathématiques du Caius College de Cambridge en 1857. Il était a élu un membre de ce collège et y est resté jusqu'à sa mort. Il a pris des ordres sacrés en 1859 et, après une brève période de travail religieux, retourne à Cambridge, où il développe des programmes en sciences morales. En plus de son travail mathématique, Venn avait un intérêt pour l'histoire et a beaucoup écrit sur son collège et famille.

Le livre de Venn, *Symbolic Logic,* clarifie les idées initialement présentées par Boole. Dans ce livre, Venn présente un développement systématique d'une méthode utilisant des figures géométriques, connues maintenant sous le nom de *diagrammes de Venn* . Aujourd'hui, ces les diagrammes sont principalement utilisés pour analyser les arguments logiques et illustrer les relations entre les ensembles. en plus à ses travaux sur la logique symbolique, Venn a apporté des contributions à la théorie des probabilités décrite dans son manuel largement utilisé sur ce sujet.

Page 142

Montrer deux ensembles sont égaux Pour montrer que deux ensembles A et B sont égaux, montrer que $A \subseteq B$ et $B \subseteq A$.

Les ensembles peuvent avoir d'autres ensembles en tant que membres. Par exemple, nous avons les ensembles

$A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ et $B = \{x \mid x$ est un sous-ensemble de l'ensemble $\{a, b\}\}$.

Notez que ces deux ensembles sont égaux, qui est, $A = B$. Notez également que $\{a\} \in A$, mais $a \notin A$.

La taille d'un ensemble

Les ensembles sont largement utilisés pour compter les problèmes, et pour de telles applications, nous devons discuter les tailles des ensembles.

DÉFINITION 4 Soit S un ensemble. S'il y a exactement n éléments distincts dans S où n est un entier non négatif, nous disons que S est un *ensemble fini* et que n est la *cardinalité* de S . La cardinalité de S est notée par $|S|$.

Remarque: Le terme *cardinalité* vient de l'utilisation courante du terme *nombre cardinal* comme la taille d'un ensemble fini.

EXEMPLE 10 Soit A l'ensemble des entiers positifs impairs inférieurs à 10. Alors $|A| = 5$.

EXEMPLE 11 Soit S l'ensemble des lettres de l'alphabet anglais. Alors $|S| = 26$.

EXEMPLE 12 Parce que l'ensemble nul n'a pas d'éléments, il s'ensuit que $|\emptyset| = 0$.

Nous nous intéresserons également aux ensembles non finis.

DÉFINITION 5 Un ensemble est dit *infini* s'il n'est pas fini.

EXEMPLE 13 L'ensemble des entiers positifs est infini.

Nous étendrons la notion de cardinalité à des ensembles infinis dans la section 2.5, un sujet difficile plein de résultats surprenants.

Ensembles de puissance

De nombreux problèmes impliquent de tester toutes les combinaisons d'éléments d'un ensemble pour voir si elles satisfont certains propriété. Pour considérer toutes ces combinaisons d'éléments d'un ensemble S, nous construisons un nouvel ensemble qui a comme ses membres tous les sous-ensembles de S.

DÉFINITION 6 Étant donné un ensemble S, l'*ensemble de puissance* de S est l'ensemble de tous les sous-ensembles de l'ensemble S. L'ensemble de puissance de S est désigné par $P(S)$.

EXEMPLE 14 Quelle est la puissance de l'ensemble $\{0, 1, 2\}$?

Solution: l' ensemble de puissance $P(\{0, 1, 2\})$ est l'ensemble de tous les sous-ensembles de $\{0, 1, 2\}$. Par conséquent,

$$P(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

Notez que l'ensemble vide et l'ensemble lui-même sont membres de cet ensemble de sous-ensembles. ▲

EXEMPLE 15 Quelle est la puissance de l'ensemble vide? Quelle est la puissance de l'ensemble $\{\emptyset\}$?

Solution: l' ensemble vide a exactement un sous-ensemble, à savoir lui-même. Par conséquent,

$$P(\emptyset) = \{\emptyset\}.$$

L'ensemble $\{\emptyset\}$ a exactement deux sous-ensembles, à savoir $\emptyset$ et l'ensemble $\{\emptyset\}$ lui-même. Donc,

$$P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}.$$ ▲

Si un ensemble a n éléments, alors son ensemble de puissance a 2^n éléments. Nous démontrerons ce fait dans plusieurs façons dans les sections suivantes du texte.

Produits cartésiens

L'ordre des éléments d'une collection est souvent important. Parce que les ensembles ne sont pas ordonnés, un autre une structure est nécessaire pour représenter les collections ordonnées. Ceci est fourni par **ordonné *n* uplets**.

DÉFINITION 7 Le *n-tuple ordonné* $(a_1, a_2, \ldots, a_n)$ est la collection ordonnée qui a *un* $_1$ comme premier élément, *un* $_2$ en tant que deuxième élément, ..., et *un* $_n$ en tant que n ième élément.

On dit que deux n-uples ordonnés sont égaux si et seulement si chaque paire correspondante de leur éléments est égal. En d'autres termes, $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ si et seulement si $a_i = b_i$, pour $i = 1, 2, \ldots, n$. En particulier, les 2-tuples ordonnés sont appelés **paires ordonnées**. Les paires ordonnées (a, b) et (c, d) sont égaux si et seulement si $a = c$ et $b = d$. Notez que (a, b) et (b, a) ne sont pas égal à moins *que* $a = b$.

RENÉ DESCARTES (1596-1650) René Descartes est né dans une famille noble près de Tours, en France, environ 200 miles au sud-ouest de Paris. Il était le troisième enfant de la première épouse de son père; elle est décédée plusieurs jours après son naissance. En raison de la mauvaise santé de René, son père, un juge provincial, a laissé les leçons formelles de son fils glisser jusqu'à à l'âge de 8 ans, René entre au collège jésuite de La Flèche. Le recteur de l'école a pris goût à lui et lui a permis de rester au lit jusqu'à tard le matin en raison de sa santé fragile. Dès lors, Descartes a passé ses matins au lit; il considérait ces temps comme ses heures de réflexion les plus productives.

Descartes a quitté l'école en 1612, s'installant à Paris, où il a passé 2 ans à étudier les mathématiques. Il a gagné licencié en droit en 1616 de l'Université de Poitiers. À 18 ans, Descartes est devenu dégoûté d'étudier et de a décidé de voir le monde. Il a déménagé à Paris et est devenu un joueur à succès. Cependant, il s'est fatigué de vie de débauche et s'installe dans la banlieue de Saint-Germain, où il se consacre à l'étude des mathématiques. Quand son jeu des amis l'ont trouvé, il a décidé de quitter la France et d'entreprendre une carrière militaire. Cependant, il n'a jamais combattu. Un jour, alors échappant au froid dans une pièce surchauffée d'un camp militaire, il fait plusieurs rêves fiévreux, qui révèlent sa future carrière en tant que mathématicien et philosophe.

Après avoir mis fin à sa carrière militaire, il a voyagé à travers l'Europe. Il a ensuite passé plusieurs années à Paris, où il a étudié les mathématiques ics et philosophie et instruments optiques construits. Descartes a décidé de déménager en Hollande, où il a passé 20 ans à errer à travers le pays, accomplissant son travail le plus important. Pendant ce temps, il a écrit plusieurs livres, y compris les *Discours,* qui contient ses contributions à la géométrie analytique, pour laquelle il est le plus connu. Il a également apporté des contributions fondamentales à la philosophie.

En 1649, Descartes a été invitée par la reine Christina à visiter sa cour en Suède pour lui enseigner la philosophie. Bien qu'il ait été réticent à vivre dans ce qu'il appelait «le pays des ours parmi les rochers et la glace», il a finalement accepté l'invitation et s'est installé en Suède.

Malheureusement, l'hiver 1649-1650 a été extrêmement amer. Descartes a attrapé une pneumonie et est décédé à la mi-février.

Bon nombre des structures discrètes que nous étudierons dans les chapitres suivants sont basées sur la notion de *Produit cartésien* d'ensembles (du nom de René Descartes). On définit d'abord le produit cartésien de deux ensembles.

DÉFINITION 8 Soit A et B *des* ensembles. Le *produit cartésien* de A et B, noté $A \times B$, est l'ensemble de tous couples (a, b), où $a \in A$ et $b \in B$. Par conséquent,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

EXEMPLE 16 Soit A représente l'ensemble de tous les étudiants d'une université et B représente l'ensemble de tous les cours offert à l'université. Qu'est-ce que le produit cartésien $A \times B$ et comment l'utiliser?

Solution: le produit cartésien $A \times B$ est constitué de toutes les paires ordonnées de la forme (a, b), où a est étudiant à l'université et b est un cours offert à l'université. Une façon d'utiliser l'ensemble $A \times B$ doit représenter toutes les inscriptions possibles d'étudiants aux cours à l'université. ▲

EXEMPLE 17 Quel est le produit cartésien de $A = \{1, 2\}$ et $B = \{a, b, c\}$?

Solution: Le produit cartésien $A \times B$ est

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

▲

Notez que les produits cartésiens $A \times B$ et $B \times A$ ne sont pas égaux, sauf si $A = \emptyset$ ou $B = \emptyset$ (de sorte que $A \times B = \emptyset$) ou $A = B$ (voir exercices 31 et 38). Ceci est illustré dans l'exemple 18.

EXEMPLE 18 Montrer que le produit cartésien $B \times A$ n'est pas égal au produit cartésien $A \times B$, où A et B sont comme dans l'exemple 17.

Solution: Le produit cartésien $B \times A$ est

$$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

Ce n'est pas égal à $A \times B$, qui a été trouvé dans l'exemple 17. ▲

Le produit cartésien de plus de deux ensembles peut également être défini.

DÉFINITION 9 Le *produit cartésien* des ensembles $A_1, A_2, \ldots, A_n$, noté $A_1 \times A_2 \times \cdots \times A_n$, est le ensemble de n-tuples ordonnés $(a_1, a_2, \ldots, a_n)$, où a_i appartient à A_i pour $i = 1, 2, \ldots, n$. En d'autre mots,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ pour } i = 1, 2, \ldots, n\}.$$

EXEMPLE 19 Quel est le produit cartésien $A \times B \times C$, où $A = \{0, 1\}$, $B = \{1, 2\}$ et $C = \{0, 1, 2\}$?

Solution: Le produit cartésien $A \times B \times C$ se compose de tous les triplets ordonnés (a, b, c), où $a \in A$, $b \in B$, et $c \in C$. Par conséquent,

$$A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2), (0, 2, 0), (0, 2, 1), (0, 2, 2), (1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}.$$

▲

Remarque: Notez que lorsque A, B et C sont des ensembles, $(A \times B) \times C$ n'est pas identique à $A \times B \times C$ (voir Exercice 39).

Nous utilisons la notation A^2 pour désigner $A \times A$, le produit cartésien de l'ensemble A avec lui-même. De même, $A^3 = A \times A \times A$, $A^4 = A \times A \times A \times A$, etc. Plus généralement,

$$A^n = \{(a_1, a_2, ..., a_n) \mid a_i \in A \text{ pour } i = 1, 2, ..., n\}.$$

EXEMPLE 20 Supposons que $A = \{1, 2\}$. Il s'ensuit que $A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ et $A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$. ▲

Un sous-ensemble R du produit cartésien $A \times B$ est appelé une **relation** de l'ensemble A à l'ensemble B. Les éléments de R sont des paires ordonnées, où le premier élément appartient à A et le second à B. Par exemple, $R = \{(a, 0), (a, 1), (a, 3), (b, 1), (b, 2), (c, 0), (c, 3)\}$ est un relation de la définissez $\{a, b, c\}$ sur l'ensemble $\{0, 1, 2, 3\}$. Une relation d'un ensemble A à lui - même est appelé une relation sur A.

EXEMPLE 21 Quelles sont les paires ordonnées dans la relation inférieure ou égale à, qui contient (a, b) si $a \leq b$, sur le plateau $\{0, 1, 2, 3\}$?

Solution: la paire ordonnée (a, b) appartient à R si et seulement si a et b appartiennent à $\{0, 1, 2, 3\}$ et $a \leq b$. Par conséquent, les paires ordonnées dans R sont (0,0), (0,1), (0,2), (0,3), (1,1), (1,2), (1,3), (2,2), (2, 3) et (3, 3). ▲

Nous étudierons longuement les relations et leurs propriétés au chapitre 9.

Utilisation de la notation d'ensemble avec des quantificateurs

Parfois, nous restreignons explicitement le domaine d'une instruction quantifiée en utilisant un notation particulière. Par exemple, $\forall x \in S\, (P(x))$ désigne la quantification universelle de $P(x)$ sur tous les éléments de l'ensemble S. En d'autres termes, $\forall x \in S\, (P(x))$ est l'abréviation de $\forall x\, (x \in S \rightarrow P(x))$. De même, $\exists x \in S\, (P(x))$ désigne la quantification existentielle de $P(x)$ au-dessus de tous les éléments de S. Autrement dit, $\exists x \in S\, (P(x))$ est l'abréviation de $\exists x\, (x \in S \wedge P(x))$.

EXEMPLE 22 Que signifient les énoncés $\forall x \in \mathbf{R}\, (x^2 \geq 0)$ et $\exists x \in \mathbf{Z}\, (x^2 = 1)$?

Solution: L'instruction $\forall x \in \mathbf{R}\, (x^2 \geq 0)$ indique que pour chaque nombre réel x, $x^2 \geq 0$. Cet état- ment peut être exprimé comme «le carré de chaque nombre réel est non négatif». déclaration.

L'instruction $\exists x \in \mathbf{Z}\, (x^2 = 1)$ indique qu'il existe un entier x tel que $x^2 = 1$. Ce peut être exprimée par «Il y a un entier dont le carré est 1.» C'est aussi une vraie déclaration parce que $x = 1$ est un entier tel que -1. ▲

Ensembles de vérité et quantificateurs

Nous allons maintenant relier les concepts de la théorie des ensembles et de la logique des prédicats. Étant donné un prédicat P, et un domaine D, nous définissons l'**ensemble** de **vérité** de P comme l'ensemble des éléments x dans D pour lesquels $P(x)$ est vrai. L'ensemble de vérité de $P(x)$ est noté $\{x \in D \mid P(x)\}$.

EXEMPLE 23 Quels sont les ensembles de vérité des prédicats $P(x)$, $Q(x)$ et $R(x)$, où le domaine est l'ensemble de entiers et $P(x)$ est «$|x| = 1$," $Q(x)$ est" $x^2 = 2$ ", et $R(x)$ est" $|x| = x$. "

Solution: l'ensemble de vérité de P, $\{x \in \mathbf{Z} \mid |x| = 1\}$, est l'ensemble des entiers pour lesquels $|x| = 1$. Parce que $|x| = 1$ lorsque $x = 1$ ou $x = -1$, et pour aucun autre entier x, nous voyons que l'ensemble de vérité de P est le définissez $\{-1, 1\}$.

L'ensemble de vérité de Q, $\{x \in \mathbf{Z} \mid x^2 = 2\}$, est l'ensemble des entiers pour lesquels $x^2 = 2$. C'est le ensemble vide car il n'y a pas d'entiers x pour lesquels $x^2 = 2$.

L'ensemble de vérité de R, $\{x \in \mathbf{Z} \mid |x| = x\}$, est l'ensemble des entiers pour lesquels $|x| = x$. Car $|x| = x$ si et seulement si $x \geq 0$, il s'ensuit que l'ensemble de vérité de R est $\mathbf{N}$, l'ensemble de non négatif entiers. ▲

Notez que $\forall x P(x)$ est vrai sur le domaine U si et seulement si l'ensemble de vérité de P est l'ensemble U. De même, $\exists x P(x)$ est vrai sur le domaine U si et seulement si l'ensemble de vérité de P n'est pas vide.

Des exercices

1. Énumérez les membres de ces ensembles.
- **a)** $\{x \mid x$ est un nombre réel tel que $x^2 = 1\}$
- **b)** $\{x \mid x$ est un entier positif inférieur à $12\}$
- **c)** $\{x \mid x$ est le carré d'un entier et $x < 100\}$
- **d)** $\{x \mid x$ est un entier tel que $x^2 = 2\}$

2. Utilisez la notation set builder pour donner une description de ces ensembles.
- **a)** $\{0, 3, 6, 9, 12\}$
- **b)** $\{-3, -2, -1, 0, 1, 2, 3\}$
- **c)** $\{m, n, o, p\}$

3. Pour chacune de ces paires d'ensembles, déterminez si le premier est un sous-ensemble du second, le second est un sous-ensemble du premier, ou aucun n'est un sous-ensemble de l'autre.
- **a)** l'ensemble des vols des compagnies aériennes de New York à New Delhi, l'ensemble des vols sans escale de New York à New Delhi
- **b)** l'ensemble des personnes qui parlent anglais, l'ensemble des personnes qui parle chinois
- **c)** l'ensemble des écureuils volants, l'ensemble des créatures vivantes qui peut voler

4. Pour chacune de ces paires d'ensembles, déterminez si le premier est un sous-ensemble du second, le second est un sous-ensemble du premier, ou aucun n'est un sous-ensemble de l'autre.
- **a)** l'ensemble des personnes qui parlent anglais, l'ensemble des personnes qui parle anglais avec un accent australien
- **b)** l'ensemble des fruits, l'ensemble des agrumes
- **c)** l'ensemble des étudiants qui étudient les mathématiques discrètes, ensemble d'étudiants étudiant les structures de données

5. Déterminez si chacune de ces paires d'ensembles est égale.
- **a)** $\{1, 3, 3, 3, 5, 5, 5, 5, 5\}$, $\{5, 3, 1\}$
- **b)** $\{\{1\}\}$, $\{1, \{1\}\}$
- **c)** $\emptyset$, $\{\emptyset\}$

6. Supposons que $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$ et $D = \{4, 6, 8\}$. Déterminer lesquels de ces ensembles sont des sous-ensembles dont autres de ces ensembles.

7. Pour chacun des ensembles suivants, déterminez si 2 est un élément de cet ensemble.
- **a)** $\{x \in \mathbf{R} \mid x$ est un entier supérieur à $1\}$
- **b)** $\{x \in \mathbf{R} \mid x$ est le carré d'un entier$\}$
- **c)** $\{2, \{2\}\}$
- **d)** $\{\{2\}, \{\{2\}\}\}$
- **e)** $\{\{2\}, \{2, \{2\}\}\}$
- **f)** $\{\{\{2\}\}\}$

8. Pour chacun des ensembles de l'exercice 7, déterminez si $\{2\}$ est un élément de cet ensemble.

9. Déterminez si chacune de ces affirmations est vraie ou faux.
- **a)** $0 \in \emptyset$
- **b)** $\emptyset \in \{0\}$
- **c)** $\{0\} \subset \emptyset$
- **d)** $\emptyset \subset \{0\}$
- **e)** $\{0\} \in \{0\}$
- **f)** $\{0\} \subset \{0\}$
- **g)** $\{\emptyset\} \subseteq \{\emptyset\}$

10. Déterminez si ces affirmations sont vraies ou fausses.
- **a)** $\emptyset \in \{\emptyset\}$
- **b)** $\emptyset \in \{\emptyset, \{\emptyset\}\}$
- **c)** $\{\emptyset\} \in \{\emptyset\}$
- **d)** $\{\emptyset\} \in \{\{\emptyset\}\}$
- **e)** $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$
- **f)** $\{\{\emptyset\}\} \subset \{\emptyset, \{\emptyset\}\}$
- **g)** $\{\{\emptyset\}\} \subset \{\{\emptyset\}, \{\emptyset\}\}$

11. Déterminez si chacune de ces affirmations est vraie ou faux.
- **a)** $x \in \{x\}$
- **b)** $\{x\} \subseteq \{x\}$
- **c)** $\{x\} \in \{x\}$
- **d)** $\{x\} \in \{\{x\}\}$
- **e)** $\emptyset \subseteq \{x\}$
- **f)** $\emptyset \in \{x\}$

12. Utilisez un diagramme de Venn pour illustrer le sous-ensemble d'entiers impairs dans l'ensemble de tous les entiers positifs ne dépassant pas 10.

13. Utilisez un diagramme de Venn pour illustrer l'ensemble de tous les mois de l'année dont les noms ne contiennent pas la lettre R dans le ensemble de tous les mois de l'année.

14. Utilisez un diagramme de Venn pour illustrer la relation $A \subseteq B$ et $B \subseteq C$.

15. Utilisez un diagramme de Venn pour illustrer les relations $A \subset B$ et $B \subset C$.

16. Utilisez un diagramme de Venn pour illustrer les relations $A \subset B$ et $A \subset C$.

17. Supposons que A, B et C sont des ensembles tels que $A \subseteq B$ et $B \subseteq C$. Montrer que $A \subseteq C$.

18. Trouver deux ensembles A et B tel que $A \in B$ et $A \subseteq B$.

19. Quelle est la cardinalité de chacun de ces ensembles?

a) $\{ a \}$ **b)** $\{\{ a \}\}$
c) $\{ a, \{ a \}\}$ **d)** $\{ a, \{ a \} , \{ a, \{ a \}\}\}$

20. Quelle est la cardinalité de chacun de ces ensembles?

a) $\emptyset$ **b)** $\{\emptyset\}$
c) $\{\emptyset , \{\emptyset\}\}$ **d)** $\{\emptyset , \{\emptyset\} , \{\emptyset , \{\emptyset\}\}\}$

21. Trouvez l'ensemble de puissance de chacun de ces ensembles, où a et b sont des éléments distincts.

a) $\{ a \}$ **b)** $\{ a, b \}$ **c)** $\{\emptyset , \{\emptyset\}\}$

22. Pouvez-vous conclure que $A = B$ si A et B sont deux ensembles avec le même ensemble de puissance?

23. Combien d'éléments chacun de ces ensembles contient-il a et b sont des éléments distincts?

a) $P (\{ a, b, \{ a, b \}\})$
b) $P (\{\emptyset , a, \{ a \} , \{\{ a \}\}\})$
c) $P (P (\emptyset))$

24. Déterminez si chacun de ces ensembles est l'ensemble de puissance de un ensemble, où a et b sont des éléments distincts.

a) $\emptyset$ **b)** $\{\emptyset , \{ a \}\}$
c) $\{\emptyset , \{ a \} , \{\emptyset , a \}\}$ **d)** $\{\emptyset , \{ a \} , \{ b \} , \{ a, b \}\}$

25. Démontrer que $P (A) \subseteq P (B)$ si et seulement si $A \subseteq B$.

26. Montrer que si $A \subseteq C$ et $B \subseteq D$, alors $A \times B \subseteq C \times D$

27. Soit $A = \{ a, b, c, d \}$ et $B = \{ y, z \}$. Trouver

a) $A \times B$. **b)** $B \times A$.

28. Quel est le produit cartésien $A \times B$, où A est l'ensemble des cours offerts par le département de mathématiques à un université et B est l'ensemble des professeurs de mathématiques à cette université? Donnez un exemple de la façon dont cette cartésienne produit peut être utilisé.

29. Quel est le produit cartésien $A \times B \times C$, où A est l'ensemble de toutes les compagnies aériennes et B et C sont à la fois l'ensemble de tous aux États-Unis? Donnez un exemple de la façon dont cela Un produit cartésien peut être utilisé.

30. Supposons que $A \times B = \emptyset$, où A et B sont des ensembles. Quoi pouvez-vous conclure?

31. Soit A un ensemble. Montrez que $\emptyset \times A = A \times \emptyset = \emptyset$.

32. Soit $A = \{ a, b, c \}$, $B = \{ x, y \}$ et $C = \{0 , 1\}$. Trouver

a) $A \times B \times C$. **b)** $C \times B \times A$.
c) $C \times A \times B$. **d)** $B \times B \times B$.

33. Trouvez A^2 si

a) $A = \{0 , 1 , 3\}$. **b)** $A = \{1 , 2 , a, b \}$.

34. Trouvez A^3 si

a) $A = \{ a \}$. **b)** $A = \{0 , a \}$.

35. Combien d'éléments différents $A \times B$ a-t-il si A a m éléments et B a n éléments?

36. Combien d'éléments différents $A \times B \times C$ a-t-il si A a m éléments, B a n éléments et C a p éléments?

37. Combien d'éléments différents A^n avoir quand A a m éléments et n est un entier positif?

38. Montrez que $A \times B = B \times A$, lorsque A et B *ne* sont pas vides, sauf si $A = B$.

39. Expliquez pourquoi $A \times B \times C$ et $(A \times B) \times C$ ne sont pas les même.

40. Expliquez pourquoi $(A \times B) \times (C \times D)$ et $A \times (B \times C) \times D$ ne sont pas les mêmes.

41. Traduisez chacune de ces quantifications en anglais et déterminer sa valeur de vérité.

a) $\forall x \in \mathbf{R}\ (x^2 = -1)$ **b)** $\exists x \in \mathbf{Z}\ (x^2 = 2)$
c) $\forall x \in \mathbf{Z}\ (x^2 > 0)$ **d)** $\exists x \in \mathbf{R}\ (x^2 = x)$

42. Traduisez chacune de ces quantifications en anglais et déterminer sa valeur de vérité.

a) $\exists x \in \mathbf{R}\ (x^3 = -1)$ **b)** $\exists x \in \mathbf{Z}\ (x + 1 > x)$
c) $\forall x \in \mathbf{Z}\ (x - 1 \in \mathbf{Z})$ **d)** $\forall x \in \mathbf{Z}\ (x^2 \in \mathbf{Z})$

43. Trouvez l'ensemble de vérité de chacun de ces prédicats où le domaine est l'ensemble des entiers.

a) $P (x) : x^2 < 3$ **b)** $Q (x) : x^2 > x$
c) $R (x) : 2 x + 1 = 0$

44. Trouvez l'ensemble de vérité de chacun de ces prédicats où le domaine est l'ensemble des entiers.

a) $P (x) : x^3 \geq 1$ **b)** $Q (x) : x^2 = 2$
c) $R (x) : x < x^2$

∗ **45.** La propriété qui définit une paire ordonnée est que deux ou- les paires dérivées sont égales si et seulement si leurs premiers éléments sont égaux et leurs seconds éléments sont égaux. Surpris Au lieu de prendre la paire ordonnée comme un con- cept, nous pouvons construire des paires ordonnées en utilisant des notions de base de la théorie des ensembles. Montrez que si nous définissons la paire ordonnée (a, b) pour être $\{\{ a \} , \{ a, b \}\}$, alors $(a, b) = (c, d)$ si et seulement si $a = c$ et $b = d$. [*Astuce:* montrez d'abord que $\{\{ a \} , \{ a, b \}\} = \{\{ c \} , \{ c, d \}\}$ si et seulement si $a = c$ et $b = d$.]

∗ **46.** Cet exercice présente **le paradoxe de Russell** . Soit S le ensemble qui contient un ensemble x si l'ensemble x n'appartient pas à lui-même, de sorte que $S = \{ x \mid x \notin x \}$.

a) Montrer l'hypothèse que S est membre de S conduit à une contradiction.

b) Montrez l'hypothèse que S n'est pas membre de S leads à une contradiction.

Par les parties (a) et (b), il s'ensuit que l'ensemble S ne peut pas être défini une amende telle qu'elle était. Ce paradoxe peut être évité en restreignant les types d'éléments que les ensembles peuvent avoir.

∗ **47.** Décrire une procédure pour lister tous les sous-ensembles d'un fini ensemble.

Page 148

Définir les opérations

introduction

Deux ou plusieurs ensembles peuvent être combinés de différentes manières.Par exemple, en commençant par l'ensemble des majors en mathématiques de votre école et de l'ensemble des majeures en informatique de votre école, nous peut former l'ensemble des étudiants qui sont des majors en mathématiques ou en informatique, l'ensemble des les étudiants qui sont des majeures conjointes en mathématiques et en informatique, l'ensemble de tous les étudiants non spécialisation en mathématiques, etc.

DÉFINITION 1 Soit A et B *des* ensembles. L' *union* des ensembles A et B , notée $A \cup B$, est l'ensemble qui contient ces éléments qui sont soit en A ou en B , ou les deux.

Un élément x appartient à l'union des ensembles A et B si et seulement si x appartient à A ou x appartient à B . Cela nous dit que

$$A \cup B = \{ x \mid x \in A \vee x \in B \} .$$

Le diagramme de Venn représenté sur la Figure 1 représente l'union des deux ensembles A et B . La zone qui représente $A \cup B$ est la zone ombrée dans le cercle représentant A ou le cercle soit B .

Nous donnerons quelques exemples de l'union des ensembles.

EXEMPLE 1 L'union des ensembles $\{1 , 3 , 5\}$ et $\{1 , 2 , 3\}$ est l'ensemble $\{1 , 2 , 3 , 5\}$; C'est, $\{1 , 3 , 5\} \cup \{1 , 2 , 3\} = \{1 , 2 , 3 , 5\}$. ▲

EXEMPLE 2 L'union de l'ensemble de toutes les filières informatiques de votre école et de l'ensemble de toutes les matières matics majors à votre école est l'ensemble des étudiants de votre école qui se spécialisent soit en mathématiques ou en informatique (ou dans les deux). ▲

DÉFINITION 2 Soit A et B *des* ensembles. L' *intersection* des ensembles A et B , notée $A \cap B$, est l'ensemble contenant les éléments à la fois A et B .

Un élément x appartient à l'intersection des ensembles A et B si et seulement si x appartient à A et x appartient à B . Cela nous dit que

$$A \cap B = \{ x \mid x \in A \wedge x \in B \} .$$

U

UNE *B*

AB est ombré.

FIGURE 1 Diagramme de Venn du Union des A et B .

U

UNE *B*

AB est ombré.

FIGURE 2 Diagramme de Venn du Intersection de A et B .

Le diagramme de Venn montre la figure 2 représente l'intersection de deux ensembles A et B . L'ombre la zone qui est à la fois dans les cercles représentant les ensembles A et B est la zone qui représente la intersection de A et B .

Nous donnons quelques exemples d'intersection d'ensembles.

EXEMPLE 3 L'intersection des ensembles $\{1 , 3 , 5\}$ et $\{1 , 2 , 3\}$ est l'ensemble $\{1 , 3\}$; C'est, $\{1 , 3 , 5\} \cap \{1 , 2 , 3\} = \{1 , 3\}$. ▲

EXEMPLE 4 L'intersection de l'ensemble de tous les majors en informatique de votre école et de l'ensemble de tous mathématiques majeures est l'ensemble de tous les étudiants qui sont des majeures conjointes en mathématiques et en informatique science. ▲

DÉFINITION 3 Deux ensembles sont appelés *disjoints* si leur intersection est l'ensemble vide.

EXEMPLE 5 Soit $A = \{1 , 3 , 5 , 7 , 9\}$ et $B = \{2 , 4 , 6 , 8 , 10\}$. Parce que $A \cap B = \emptyset$, A et B sont disjoints. ▲

Attention à ne pas overcount!

Nous sommes souvent intéressés à trouver la cardinalité d'une union de deux ensembles finis A et B. Remarque que $|A| + |B|$ compte chaque élément qui est dans A mais pas dans B ou dans B mais pas dans A exactement une fois, et chaque élément qui est à la fois dans A et B exactement deux fois. Ainsi, si le nombre d'éléments qui sont à la fois A et B est soustrait de $|A| + |B|$, les éléments de $A \cap B$ ne seront comptés qu'une seule fois. Par conséquent,

$|A \cup B| = |A| + |B| - |A \cap B|$.

La généralisation de ce résultat aux unions d'un nombre arbitraire d'ensembles est appelée le **principe d'inclusion-exclusion** . Le principe d'inclusion-exclusion est une technique importante utilisée dans énumération. Nous discuterons de ce principe et d'autres techniques de comptage en détail dans les chapitres 6 et 8.

Il existe d'autres façons importantes de combiner des ensembles.

DÉFINITION 4 Soit A et B *des* ensembles. La *différence* de A et B, notée $A - B$, est l'ensemble contenant les des éléments qui sont en A , mais pas dans B . La différence de A et B est également appelée *complément de B par rapport à A* .

Remarque: La différence des ensembles A et B est parfois désigné par $A \setminus B$.

Un élément x appartient à la différence de A et B si et seulement si $x \in A$ et $x / \in B$. Cela nous dit cette

$A - B = \{ x \mid x \in A \wedge x / \in B \}$.

Le diagramme de Venn montre la figure 3 représente la différence des ensembles A et B . L'ombre zone à l'intérieur du cercle qui représente A et à l'extérieur du cercle qui représente B est la zone qui représente $A - B$.

Nous donnons quelques exemples de différences d'ensembles.

EXEMPLE 6 La différence de $\{1, 3, 5\}$ et $\{1, 2, 3\}$ est l'ensemble $\{5\}$; c'est-à-dire $\{1, 3, 5\} - \{1, 2, 3\} = \{5\}$. Cette est différent de la différence de $\{1, 2, 3\}$ et $\{1, 3, 5\}$, qui est l'ensemble $\{2\}$. ▲

EXEMPLE 7 La différence de l'ensemble des filières informatiques de votre école et de l'ensemble des mathématiques les majors de votre école est l'ensemble de toutes les majors en informatique de votre école qui ne sont pas aussi majeures mathématiques. ▲

U

UNE B

A - B est ombré.

FIGURE 3 Diagramme de Venn pour la différence entre *A* et *B* .

U

UNE

A est ombré.

FIGURE 4 Diagramme de Venn pour le complément de l'ensemble *A* .

Une fois l'ensemble universel U spécifié, le **complément** d'un ensemble peut être défini.

DÉFINITION 5 Soit U l'ensemble universel. Le *complément* de l'ensemble A, noté A, est le complément de A par rapport à U . Par conséquent, le complément de l'ensemble A est $U - A$.

Un élément appartient à A si et seulement si $x / \in A$. Cela nous dit que

$A = \{ x \in U \mid x / \in A \}$.

Sur la figure 4 , la zone hachurée à l' extérieur du cercle représentant A est la zone qui représente A .

Nous donnons quelques exemples du complément d'un ensemble.

EXEMPLE 8 Soit $A = \{ a, e, i, o, u \}$ (où l'ensemble universel est l'ensemble des lettres de l'alphabet anglais).alors $A = \{ b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z \}$. ▲

EXEMPLE 9 Soit A l'ensemble des entiers positifs supérieur à 10 (avec l'ensemble universel l'ensemble de tous les positifs entiers). Alors $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. ▲

C'est au lecteur (Exercice 19) de montrer que l'on peut exprimer la différence de A et B comme l'intersection de A et le complément de B . C'est,

$A - B = A \cap B$.

Définir les identités

Définir les identités et
propositionnel
les équivalences sont juste
cas particuliers d'identités
pour l'algèbre booléenne.

Le tableau 1 répertorie les identités d'ensemble les plus importantes. Nous allons prouver plusieurs de ces identités ici, en utilisant trois méthodes différentes. Ces méthodes sont présentées pour illustrer qu'il existe souvent de nombreuses différentes approches pour résoudre un problème. Les preuves des identités restantes seront être laissé comme exercices. Le lecteur doit noter la similitude entre ces identités définies et les équivalences logiques discutées à la section 1.3. (Comparez le tableau 6 de la section 1.6 et le tableau 1.) En fait, les identités d'ensemble données peuvent être prouvées directement à partir des équivalences logiques correspondantes. En outre, les deux sont des cas particuliers d'identités qui valent pour l'algèbre de Boole (discuté dans Chapitre 12).

Une façon de montrer que deux ensembles sont égaux consiste à montrer que chacun est un sous-ensemble de l'autre.Rappel que pour montrer qu'un ensemble est un sous-ensemble d'un deuxième ensemble, nous pouvons montrer que si un élément appartient à le premier ensemble, alors il doit également appartenir au deuxième ensemble.Nous utilisons généralement une preuve directe pour ce faire. Nous illustrons ce type de preuve en établissant la première des lois de De Morgan.

TABLEAU 1 Définir les identités.

Identité	***Nom***
$A \cap U = A$ $A \cup \emptyset = A$	Lois sur l'identité
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Lois de domination
$A \cup A = A$ $A \cap A = A$	Lois idempotentes
$(A) = A$	Loi de complémentation
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Lois commutatives
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Lois associatives
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Lois distributives
$A \cap B = A \cup B$ $A \cup B = A \cap B$	Les lois de De Morgan
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Lois d'absorption
$A \cup A = U$ $A \cap A = \emptyset$	Lois complémentaires

Exemple 10 : Démontrer que $A \cap B = A \cup B$.

Cette identité dit que
le complément du
intersection de deux ensembles
est l'union de leur
compléments.

Solution: Nous prouverons que les deux ensembles $A \cap B$ et $A \cup B$ sont égaux en montrant que chaque ensemble est un sous-ensemble de l'autre.

Tout d' abord, nous allons montrer que $A \cap B \subseteq A \cup B$. Nous faisons cela en montrant que si x est dans $A \cap B$, alors il doit également être en $A \cup B$. Supposons maintenant que $x \in A \cap B$. Par la définition du complément, $x \in A \cap B$. En utilisant la définition de l'intersection, nous voyons que la proposition $\neg((x \in A) \wedge (x \in B))$ est vraie.

En appliquant la loi de De Morgan aux propositions, on voit que $\neg(x \in A)$ ou $\neg(x \in B)$. En utilisant la définition de la négation des propositions, nous avons $x \in A$ ou $x \in B$. Utilisation de la définition de le complément d'un ensemble, nous voyons que cela implique que $x \in A$ ou $x \in B$. Par conséquent, définition de l' union, nous voyons que $x \in A \cup B$. Nous avons montré que $A \cap B \subseteq A \cup B$.

Ensuite, nous allons montrer que $A \cup B \subseteq A \cap B$. Nous faisons cela en montrant que si x est dans $A \cup B$, alors il doit également être en A de B . Supposons maintenant que $x \in A \cup B$. Par la définition de l'union, nous savons que $x \in A$ ou $x \in B$. En utilisant la définition du complément, on voit que $x \in A$ ou $x \in B$. Par conséquent, la proposition $\neg(x \in A) \vee \neg(x \in B)$ est vraie.

Par la loi de De Morgan pour les propositions, nous concluons que $\neg((x \in A) \wedge (x \in B))$ est vrai. Par la définition de l'intersection, il s'ensuit que $\neg(x \in A \cap B)$. Nous utilisons maintenant la définition de complément à conclure que $x \in A \cap B$. Cela montre que $A \cup B \subseteq A \cap B$.

Parce que nous avons montré que chaque ensemble est un sous-ensemble de l'autre, les deux ensembles sont égaux et l'identité est prouvée. ▲

Nous pouvons exprimer plus succinctement le raisonnement utilisé dans l'exemple 10 en utilisant la notation set builder, comme l'illustre l'exemple 11.

EXEMPLE 11 Utiliser la notation de constructeur d'ensemble et les équivalences logiques pour établir la première loi De Morgan $A \cap B =$ $A \cup B$.

Solution: Nous pouvons prouver cette identité avec les étapes suivantes.

$$\begin{aligned}
A \cap B &= \{ x \mid x \notin A \cap B \} && \text{par définition de complément} \\
&= \{ x \mid \neg (x \in (A \cap B)) \} && \text{par définition de n'appartient pas au symbole} \\
&= \{ x \mid \neg (x \in A \wedge x \in B) \} && \text{par définition d'intersection} \\
&= \{ x \mid \neg (x \in A) \vee \neg (x \in B) \} && \text{par la première loi de Morgan pour les équivalences logiques} \\
&= \{ x \mid x \notin A \vee x \notin B \} && \text{par définition de n'appartient pas au symbole} \\
&= \{ x \mid x \in A \vee x \in B \} && \text{par définition de complément} \\
&= \{ x \mid x \in A \cup B \} && \text{par définition d'union} \\
&= A \cup B && \text{au sens de la notation set builder}
\end{aligned}$$

Notez qu'en plus des définitions de complément, union, set membership et set builder notation, cette preuve utilise la deuxième loi de Morgan pour les équivalences logiques. ▲

Prouver une identité d'ensemble impliquant plus de deux ensembles en montrant chaque côté de l'identité est un sous-ensemble de l'autre nécessite souvent de garder une trace des différents cas, comme l'illustre la preuve dans l'exemple 12 de l'une des lois de distribution des ensembles.

EXEMPLE 12 Démontrer la deuxième loi distributive du tableau 1, qui indique que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ pour tous les ensembles A , B et C .

Solution: Nous prouverons cette identité en montrant que chaque côté est un sous-ensemble de l'autre côté.

Supposons que $x \in A \cap (B \cup C)$. Alors $x \in A$ et $x \in B \cup C$. Par la définition de l'union, il il s'ensuit que $x \in A$ et $x \in B$ ou $x \in C$ (ou les deux). En d'autres termes, nous savons que le composé la proposition $(x \in A) \wedge ((x \in B) \vee (x \in C))$ est vraie. Par la loi distributive de conjonction sur disjonction, il s'ensuit que $((x \in A) \wedge (x \in B)) \vee ((x \in A) \wedge (x \in C))$. Nous concluons que soit $x \in A$ et $x \in B$, ou $x \in A$ et $x \in C$. Par la définition de l'intersection, il s'ensuit que $x \in A \cap B$ ou $x \in A \cap C$. En utilisant la définition de l'union, nous concluons que $x \in (A \cap B) \cup (A \cap C)$. nous conclure que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Supposons maintenant que $x \in (A \cap B) \cup (A \cap C)$. Ensuite, par la définition de l'union, $x \in A \cap B$ ou $x \in A \cap C$. Par la définition de l'intersection, il s'ensuit que $x \in A$ et $x \in B$ ou que $x \in A$ et $x \in C$. De là , nous voyons que $x \in A$ et $x \in B$ ou $x \in C$. Par conséquent, par la définition de union , nous voyons que $x \in A$ et $x \in B \cup C$. De plus, par la définition de l'intersection, il suit que $x \in A \cap (B \cup C)$. Nous concluons que $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Ceci termine la preuve de l'identité. ▲

Les identités des ensembles peuvent également être prouvées à l'aide **des tables d'appartenance** . Nous considérons chaque combinaison d'ensembles auxquels un élément peut appartenir et vérifier que les éléments dans les mêmes combinaisons d'ensembles appartiennent aux deux ensembles de l'identité. Pour indiquer qu'un élément est dans un ensemble, un 1 est utilisé; à indiquent qu'un élément n'est pas dans un ensemble, un 0 est utilisé. (Le lecteur doit noter la similitude entre tables des membres et tables de vérité.)

EXEMPLE 13 Utilisez un tableau d'appartenance pour montrer que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Solution: le tableau d'appartenance pour ces combinaisons d'ensembles est indiqué dans le tableau 2. Ce tableau a huit rangées. Étant donné que les colonnes pour $A \cap (B \cup C)$ et $(A \cap B) \cup (A \cap C)$ sont les mêmes, la l'identité est valide. ▲

Des identités d'ensemble supplémentaires peuvent être établies en utilisant celles que nous avons déjà prouvées. Considérer Exemple 14.

TABLEAU 2 **Tableau d'appartenance à la propriété distributive.**

UNE	*B*	*C*	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

EXEMPLE 14 Soit A , B et C *des* ensembles. Montre CA

$$A \cup (B \cap C) = (C \cup B) \cap A.$$

Solution: nous avons

$$\begin{aligned} A \cup (B \cap C) &= A \cap (B \cap C) && \text{par la première loi De Morgan} \\ &= A \cap (B \cup C) && \text{par la deuxième loi de De Morgan} \\ &= (B \cup C) \cap A && \text{par la loi commutative pour les intersections} \\ &= (C \cup B) \cap A && \text{par la loi commutative pour les unions.} \end{aligned}$$

▲

Unions généralisées et intersections

Du fait que les unions et les intersections d'ensembles satisfont aux lois associatives, les ensembles $A \cup B \cup C$ et $A \cap B \cap C$ sont bien définis; c'est-à-dire que la signification de cette notation est sans ambiguïté lorsque A , B et C sont des ensembles. Autrement dit, nous n'avons pas à utiliser de parenthèses pour indiquer quelle opération vient d' abord parce que $A \cup (B \cup C) = (A \cup B) \cup C$ et $A \cap (B \cap C) = (A \cap B) \cap C$. Notez que $A \cup B \cup C$ contient les éléments qui se trouvent dans au moins l'un des ensembles A, B et C, et qui $A \cap B \cap C$ contient les éléments qui sont dans l' ensemble de A , B et C . Ces combinaisons de trois ensembles, A , B et C , sont illustrés à la figure 5.

U
UNE *B*
C

(a) A U B U C est ombré.

U
UNE *B*
C

UU
(b) *ABC* est ombré.

FIGURE 5 **L'Union et l' intersection de A , B et C .**

Exemple 15 Soit $A = \{0, 2, 4, 6, 8\}$, $B = \{0, 1, 2, 3, 4\}$, et $C = \{0, 3, 6, 9\}$. Que sont $A \cup B \cup C$ et $A \cap B \cap C$?

Solution: L'ensemble $A \cup B \cup C$ contient ces éléments dans au moins un des A, B et C. Par conséquent,

$$A \cup B \cup C = \{0, 1, 2, 3, 4, 6, 8, 9\}.$$

L'ensemble $A \cap B \cap C$ contient les éléments dans tous les trois de A, B et C. Donc,

$$A \cap B \cap C = \{0\}.$$

▲

Nous pouvons également considérer les unions et les intersections d'un nombre arbitraire d'ensembles.Nous introduisons ces définitions.

DÉFINITION 6 L' *union* d'une collection d'ensembles est l'ensemble qui contient les éléments qui sont membres de au moins un ensemble dans la collection.

Nous utilisons la notation

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

pour désigner l'union des ensembles $A_1, A_2, \ldots, A_n$.

DÉFINITION 7 L' *intersection* d'une collection d'ensembles est l'ensemble qui contient les éléments qui sont membres de tous les ensembles de la collection.

Nous utilisons la notation

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

pour désigner l'intersection des ensembles $A_1, A_2, \ldots, A_n$. Nous illustrons les syndicats généralisés et intersections avec l'exemple 16.

EXEMPLE 16 Pour $i = 1, 2, \ldots$, soit $A_i = \{i, i+1, i+2, \ldots\}$. Alors,

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{1, 2, 3, \ldots\},$$

et

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{n, n+1, n+2, \ldots\} = A_n.$$

▲

Nous pouvons étendre la notation que nous avons introduite pour les unions et les intersections à d'autres familles de ensembles. En particulier, nous utilisons la notation

$$A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots = \bigcup_{i=1}^{\infty} A_i$$

pour désigner l'union des ensembles $A_1, A_2, \ldots, A_n, \ldots$. De même, l'intersection de ces ensembles est dénoté par

$$A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots = \bigcap_{i=1}^{\infty} A_i.$$

Plus généralement, quand *je suis* un ensemble, les notations $\bigcap_{i \in I} A_i$ et $\bigcup_{i \in I} A_i$ sont utilisés pour désigner l'intersection et l'union des ensembles A_i pour $i \in I$, respectivement. Notez que nous avons $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I\,(x \in A_i)\}$ et $\bigcup_{i \in I} A_i = \{x \mid \exists i \in I\,(x \in A_i)\}$.

EXEMPLE 17 On suppose que $A_i = \{1, 2, 3, \ldots, i\}$ pour $i = 1, 2, 3, \ldots$. Alors,

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \{1, 2, 3, \ldots\} = \mathbf{Z}^+$$

et

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{1, 2, 3, \ldots, i\} = \{1\}.$$

Pour voir que l'union de ces ensembles est l'ensemble d'entiers positifs, notez que chaque positif l'entier n est dans au moins l'un des ensembles, car il appartient à $A_n = \{1, 2, \ldots, n\}$, et à chaque élément des ensembles dans l'union est un entier positif. Pour voir que l'intersection de ces ensembles est l'ensemble $\{1\}$, notez que le seul élément qui appartient à tous les ensembles $A_1, A_2, \ldots$ est 1. Pour voir cette note qui $A_1 = \{1\}$ et $1 \in A_i$ pour $i = 1, 2, \ldots$. ▲

Représentation informatique des ensembles

Il existe différentes façons de représenter des ensembles à l'aide d'un ordinateur. Une méthode consiste à stocker les éléments de l'ensemble d'une manière non ordonnée. Cependant, si cela est fait, les opérations de calcul de la l'union, l'intersection ou la différence de deux ensembles prendrait du temps, car chacun de ces les opérations nécessiteraient une grande quantité de recherche d'éléments. Nous présenterons une méthode pour stocker des éléments en utilisant un ordre arbitraire des éléments de l'ensemble universel. Cette méthode de représenter les ensembles facilite le calcul des combinaisons d'ensembles.

Supposons que l'ensemble universel U est fini (et de taille raisonnable pour que le nombre de éléments de U ne dépasse pas la taille de la mémoire de l'ordinateur utilisé). Tout d'abord, spécifiez un ordre arbitraire des éléments de U, par exemple $a_1, a_2, \ldots, a_n$. Représenter un sous-ensemble A de U avec la chaîne de bits de longueur n, où le i ème bit de cette chaîne est 1 si a_i appartient à A et vaut 0 si *un* $_i$ ne fait pas partie A. L'exemple 18 illustre cette technique.

EXEMPLE 18 Soit $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, et l'ordre des éléments de U a les éléments dans ordre croissant; c'est-à-dire $a_i = i$. Quelles chaînes de bits représentent le sous-ensemble de tous les entiers impairs dans U, le sous-ensemble de tous les entiers pairs dans U, et le sous-ensemble d'entiers ne dépassant pas 5 dans U ?

Solution: la chaîne de bits qui représente l'ensemble des entiers impairs dans U, *à* savoir $\{1, 3, 5, 7, 9\}$, a un bit en première, troisième, cinquième, septième et neuvième positions, et un zéro ailleurs. Il est

$$10\ 1010\ 1010.$$

(Nous avons divisé cette chaîne de bits de longueur dix en blocs de longueur quatre pour une lecture facile.) De même, nous représentons le sous-ensemble de tous les entiers pairs dans U, *à* savoir $\{2, 4, 6, 8, 10\}$, par la chaîne

01 0101 0101 .

L'ensemble de tous les entiers dans U qui ne dépassent pas 5, à savoir $\{1, 2, 3, 4, 5\}$, est représenté par le chaîne

11 1110 0000 .

▲

En utilisant des chaînes de bits pour représenter des ensembles, il est facile de trouver des compléments d'ensembles et d'unions, sections et différences d'ensembles. Pour rechercher la chaîne de bits pour le complément d'un ensemble à partir du bit chaîne pour cet ensemble, nous changeons simplement chaque 1 en 0 et chaque 0 en 1, car $x \in A$ si et seulement si $x \notin A$. Notez que cette opération correspond à prendre la négation de chaque bit lorsque l'on associe un bit avec une valeur de vérité - avec 1 représentant vrai et 0 représentant faux.

EXEMPLE 19 Nous avons vu que la chaîne de bits pour l'ensemble $\{1, 3, 5, 7, 9\}$ (avec l'ensemble universel $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$) est

10 1010 1010 .

Quelle est la chaîne de bits pour le complément de cet ensemble?

Solution: la chaîne de bits pour le complément de cet ensemble est obtenue en remplaçant 0s par 1s et vice versa. Cela donne la chaîne

01 0101 0101 ,

ce qui correspond à l'ensemble $\{2, 4, 6, 8, 10\}$.

▲

Pour obtenir la chaîne de bits pour l'union et l'intersection de deux ensembles, nous effectuons un booléen au niveau du bit opérations sur les chaînes de bits représentant les deux ensembles.Le bit en i ème position de la chaîne de bits de l'union est 1 si l'un des bits en i ème position dans les deux chaînes est 1 (ou les deux sont 1), et est 0 lorsque les deux bits sont 0. Par conséquent, la chaîne de bits pour l'union est le *OU au niveau* du bit des chaînes de bits pour les deux ensembles. Le bit en i ème position de la chaîne de bits de l'intersection est 1 lorsque les bits dans la position correspondante dans les deux chaînes sont à la fois 1 et 0 lorsque l'un des deux bits est 0 (ou les deux le sont).Par conséquent, la chaîne de bits pour l'intersection est le bit au niveau *ET* des chaînes de bits pour les deux ensembles.

EXEMPLE 20 Les chaînes de bits pour les ensembles $\{1, 2, 3, 4, 5\}$ et $\{1, 3, 5, 7, 9\}$ sont 11 1110 0000 et 10 1010 1010, respectivement. Utilisez des chaînes de bits pour trouver l'union et l'intersection de ces ensembles.

Solution: la chaîne de bits pour l'union de ces ensembles est

$$11\ 1110\ 0000 \vee 10\ 1010\ 1010 = 11\ 1110\ 1010,$$

ce qui correspond à l'ensemble $\{1, 2, 3, 4, 5, 7, 9\}$. La chaîne de bits pour l'intersection de ces ensembles est

$$11\ 1110\ 0000 \wedge 10\ 1010\ 1010 = 10\ 1010\ 0000,$$

ce qui correspond à l'ensemble $\{1, 3, 5\}$.

▲

Des exercices

1. Soit A l'ensemble des étudiants qui vivent dans un rayon d'un mile de l'école et laissez B être l'ensemble des élèves qui marchent vers Des classes. Décrivez les élèves dans chacun de ces ensembles.

a) $A \cap B$ **b)** $A \cup B$
c) $A - B$ **d)** $B - A$

2. Supposons que A est l'ensemble des étudiants de deuxième année de votre école et B est l'ensemble des étudiants en mathématiques discrètes à votre école. Exprimez chacun de ces ensembles en termes de A et B .

a) l'ensemble des étudiants de deuxième année prenant des mathématiques discrètes votre école
b) l'ensemble des étudiants de deuxième année de votre école qui ne ing mathématiques discrètes
c) l'ensemble des élèves de votre école qui sont soit moeurs ou prennent des mathématiques discrètes
d) l'ensemble des élèves de votre école qui ne sont pas non plus étudiants de deuxième année ou ne prennent pas de mathématiques discrètes

3. Soit $A = \{1, 2, 3, 4, 5\}$ et $B = \{0, 3, 6\}$. Trouver

a) $A \cup B$. **b)** $A \cap B$.

b) à l' aide d'une table des membres.

16. Soit A et B *des* ensembles. Montre CA

a) $(A \cap B) \subseteq A$. **b)** $A \subseteq (A \cup B)$.
c) $A - B \subseteq A$. **d)** $A \cap (B - A) = \emptyset$.
e) $A \cup (B - A) = A \cup B$.

17. Montrer que si A , B et C sont des ensembles, alors $A \cap B \cap C = A \cup B \cup C$

a) en montrant chaque côté est un sous-ensemble de l'autre côté.
b) à l' aide d'une table des membres.

18. Soit A , B et C *des* ensembles. Montre CA

a) $(A \cup B) \subseteq (A \cup B \cup C)$.
b) $(A \cap B \cap C) \subseteq (A \cap B)$.
c) $(A - B) - C \subseteq A - C$.
d) $(A - C) \cap (C - B) = \emptyset$.
e) $(B - A) \cup (C - A) = (B \cup C) - A$.

19. Montrez que si A et B sont des ensembles, alors

a) $A - B = A \cap B$.
b) $(A \cap B) \cup (A \cap B) = A$.

20. Montrer que si A et B sont des ensembles avec $A \subseteq B$, alors

c) $A - B$ **d)** $B - A$.

4. Soit $A = \{ a, b, c, d, e \}$ et $B = \{ a, b, c, d, e, f, g, h \}$.
Trouver

a) $A \cup B$. **b)** $A \cap B$.
c) $A - B$. **d)** $B - A$.

Dans les exercices 5 à 10, supposez que A est un sous-ensemble de certains ing ensemble universel U .

5. Prouvez la loi de complémentation du tableau 1 en montrant que $A = A$.

6. Prouvez les lois sur l'identité du tableau 1 en montrant que

a) $A \cup \emptyset = A$. **b)** $A \cap U = A$.

7. Prouvez les lois de domination du tableau 1 en montrant que

a) $A \cup U = U$. **b)** $A \cap \emptyset = \emptyset$.

8. Prouvez les lois idempotentes du tableau 1 en montrant que

a) $A \cup A = A$. **b)** $A \cap A = A$.

9. Prouvez les lois complémentaires du tableau 1 en montrant que

a) $A \cup A = U$. **b)** $A \cap A = \emptyset$.

10. Montrez que

a) $A - \emptyset = A$. **b)** $\emptyset - A = \emptyset$.

11. Soit A et B *des* ensembles. Démontrer les lois commutatives de Tableau 1 en montrant que

a) $A \cup B = B \cup A$.
b) $A \cap B = B \cap A$.

12. Démontrez la première loi d'absorption du tableau 1 en montrant que si A et B sont des ensembles, alors $A \cup (A \cap B) = A$.

13. Démontrer la deuxième loi d'absorption du tableau 1 en montrant que si A et B sont des ensembles, alors $A \cap (A \cup B) = A$.

14. Trouvez les ensembles A et B si $A - B = \{1 , 5 , 7 , 8\}$, $B - A = \{2 , 10\}$ et $A \cap B = \{3 , 6 , 9\}$.

15. Prouvez la deuxième loi De Morgan dans le tableau 1 en montrant que si A et B sont des ensembles, alors $A \cup B = A \cap B$

a) en montrant chaque côté est un sous-ensemble de l'autre côté.

a) $A \cup B = B$.
b) $A \cap B = A$.

21. Démontrez la première loi associative du tableau 1 en que si A , B et C sont des ensembles, alors $A \cup (B \cup C) = (A \cup B) \cup C$.

22. Démontrez la deuxième loi associative du tableau 1 en montrant que si A , B et C sont des ensembles, alors $A \cap (B \cap C) = (A \cap B) \cap C$.

23. Démontrez la première loi de répartition du tableau 1 en que si A , B et C sont des ensembles, alors $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

24. Soit A , B et C *des* ensembles. Montrez que $(A - B) - C = (A - C) - (B - C)$.

25. Soit $A = \{0 , 2 , 4 , 6 , 8 , 10\}$, $B = \{0 , 1 , 2 , 3 , 4 , 5 , 6\}$ et $C = \{4 , 5 , 6 , 7 , 8 , 9 , 10\}$. Trouver

a) $A \cap B \cap C$. **b)** $A \cup B \cup C$.
c) $(A \cup B) \cap C$. **d)** $(A \cap B) \cup C$.

26. Dessinez les diagrammes de Venn pour chacune de ces combinaisons des ensembles A , B et C .

a) $A \cap (B \cup C)$ **b)** $A \cap B \cap C$
c) $(A - B) \cup (A - C) \cup (B - C)$

27. Dessinez les diagrammes de Venn pour chacune de ces combinaisons des ensembles A , B et C .

a) $A \cap (B - C)$ **b)** $(A \cap B) \cup (A \cap C)$
c) $(A \cap B) \cup (A \cap C)$

28. Dessinez les diagrammes de Venn pour chacune de ces combinaisons des ensembles A , B , C et D .

a) $(A \cap B) \cup (C \cap D)$ **b)** $A \cup B \cup C \cup D$
c) $A - (B \cap C \cap D)$

29. Que pouvez-vous dire des ensembles A et B si nous savons que

a) $A \cup B = A$? **b)** $A \cap B = A$?
c) $A - B = A$? **d)** $A \cap B = B \cap A$?
e) $A - B = B - A$?

30. Pouvez-vous conclure que $A = B$ si A , B et C sont des ensembles tels cette

a) $A \cup C = B \cup C$? **b)** $A \cap C = B \cap C$?
c) $A \cup C = B \cup C$ et $A \cap C = B \cap C$?

31. Soit A et B des sous - ensembles d'un ensemble universel U . Montre CA $A \subseteq B$ si et seulement si $B \subseteq A$.

La **différence symétrique** de A et B , notée $A \oplus B$, est l'ensemble contenant ces éléments dans A ou B , mais pas dans à la fois A et B .

32. Trouvez la différence symétrique de $\{1 , 3 , 5\}$ et $\{1 , 2 , 3\}$.

33. Trouvez la différence symétrique de l'ensemble des sci- majeures dans une école et l'ensemble des majeures mathématiques dans cette école.

34. Tracez un diagramme de Venn pour la différence symétrique du ensembles A et B .

35. Montrer que $A \oplus B = (A \cup B) - (A \cap B)$.

36. Montrez que $A \oplus B = (A - B) \cup (B - A)$.

37. Montrer que si A est un sous-ensemble d'un ensemble universel U , alors

a) $A \oplus A = \emptyset$. **b)** $A \oplus \emptyset = A$.
c) $A \oplus U = A$. **d)** $A \oplus A = U$.

38. Montrez que si A et B sont des ensembles, alors

a) $A \oplus B = B \oplus A$. **b)** $(A \oplus B) \oplus B = A$.

39. Que pouvez-vous dire des ensembles A et B si $A \oplus B = A$?

∗ **40.** Déterminer si la différence symétrique est associée

tive; c'est-à-dire, si A , B et C sont des ensembles, cela signifie-t-il que $A \oplus (B \oplus C) = (A \oplus B) \oplus C$?

∗ **41.** Supposons que A , B et C sont des ensembles tels que $A \oplus C = B \oplus C$. Faut-il que ce soit $A = B$?

42. Si A, B, C et D sont des ensembles, cela signifie-t-il que $(A \oplus B) \oplus (C \oplus D) = (A \oplus C) \oplus (B \oplus D)$?

43. Si A , B , C et D sont des ensembles, cela signifie-t-il que $(A \oplus B) \oplus (C \oplus D) = (A \oplus D) \oplus (B \oplus C)$?

44. Montrer que si A et B sont des ensembles finis, alors $A \cup B$ est un ensemble fini

49. Soit A_i l'ensemble de toutes les chaînes de bits non vides (c'est-à-dire le bit chaînes de longueur d'au moins un) d'une longueur ne dépassant pas i .
Trouver

une) $\bigcup_{i=1} A_i$. **b)** $\bigcap_{i=1} A_i$.

50. Trouver $\bigcup_{i=1}^{\infty} A_i$ et $\bigcap_{i=1}^{\infty} A_i$ si pour chaque entier positif i ,

a) $A_i = \{ i, i+1 , i+2 , ... \}$.

b) $A_i = \{0 , i \}$.

c) $A_i = (0 , i)$, c'est-à-dire l'ensemble des nombres réels x avec $0 < x < i$.

d) $A_i = (i, \infty)$, c'est-à-dire l'ensemble des nombres réels x avec $x > i$.

51. Trouver $\bigcup_{i=1}^{\infty} A_i$ et $\bigcap_{i=1}^{\infty} A_i$ si pour chaque entier positif i ,

a) $A_i = \{- i, - i + 1 , ..., -1 , 0 , 1 , ..., i - 1 , i \}$.

b) $A_i = \{- i, i \}$.

c) $A_i = [- i, i]$, c'est-à-dire l'ensemble des nombres réels x avec $- i \leq x \leq i$.

d) $A_i = [i, \infty)$, c'est-à-dire l'ensemble des nombres réels x avec $x \geq i$.

52. Supposons que l'ensemble universel soit $U = \{1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10\}$. Exprimez chacun de ces ensembles avec un bit chaînes où le i ème bit de la chaîne est 1 si i est dans le définir et 0 sinon.

a) $\{3 , 4 , 5\}$

b) $\{1 , 3 , 6 , 10\}$

c) $\{2 , 3 , 4 , 7 , 8 , 9\}$

53. En utilisant le même ensemble universel que dans le dernier problème, trouvez l'ensemble spécifié par chacune de ces chaînes de bits.

a) 11 1100 1111

b) 01 0111 1000

c) 10 0000 0001

54. Quels sous-ensembles d'un ensemble universel fini ces chaînes de bits représenter?

a) la chaîne avec tous les zéros

ensemble.

45. Montrez que si A est un ensemble infini, alors chaque fois que B est un ensemble, $A \cup B$ est également un ensemble infini.

∗ **46.** Montrez que si A , B et C sont des ensembles, alors

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

(Il s'agit d'un cas particulier du principe d'inclusion-exclusion qui sera étudiée au chapitre 8.)

47. Soit $A_i = \{1, 2, 3, ..., i\}$ pour $i = 1, 2, 3, ...$ Trouver

une) $\bigcup_{i=1}^{\infty} A_i$. **b)** $\bigcap_{i=1}^{\infty} A_i$.

48. Soit $A_i = \{..., -2, -1, 0, 1, ..., i\}$. Trouver

une) $\bigcup_{i=1}^{\infty} A_i$. **b)** $\bigcap_{i=1}^{\infty} A_i$.

b) la chaîne avec tous ceux

55. Quelle est la chaîne de bits correspondant à la différence de deux jeux?

56. Quelle est la chaîne de bits correspondant à la différence symétrique différence de deux ensembles?

57. Montrez comment les opérations au niveau du bit sur les chaînes de bits peuvent être utilisé pour trouver ces combinaisons de $A = \{a, b, c, d, e\}$, $B = \{b, c, d, g, p, t, v\}$, $C = \{c, e, i, o, u, x, y, z\}$ et $D = \{d, e, h, i, n, o, t, u, x, y\}$.

a) $A \cup B$ **b)** $A \cap B$

c) $(A \cup D) \cap (B \cup C)$ **d)** $A \cup B \cup C \cup D$

58. Comment l'union et l'intersection de n ensembles qui sont tous trouver des sous-ensembles de l'ensemble universel U à l'aide de chaînes de bits?

Le **successeur** de l'ensemble A est l'ensemble $A \cup \{A\}$.

59. Trouvez les successeurs des ensembles suivants.

a) $\{1, 2, 3\}$ **b)** $\emptyset$

c) $\{\emptyset\}$ **d)** $\{\emptyset, \{\emptyset\}\}$

60. Combien d'éléments le successeur d'un ensemble avec n éléments ont?

Parfois, le nombre de fois qu'un élément se produit dans un questions de collection non ordonnées. **Les multisets** sont des **collectes** non ordonnées des éléments où un élément peut apparaître en tant que membre plus d'une fois. La notation $\{m_1 \cdot a_1, m_2 \cdot a_2, ..., m_r \cdot a_r\}$ désigne le multiset avec l'élément a_1 apparaissant m_1 fois, element *un* $_2$ se produisant m_2 fois, et ainsi de suite. Les nombres m_i, $i = 1, 2, ..., r$ sont appelés les **multiplicités** des éléments a_i, $i = 1, 2, ..., r$.

Soit P et Q *des* multisets. L' **union** des multisets P et Q est le multiset où la multiplicité d'un élément est au maximum de ses multiplicités de P et Q . L' **intersection** **tion** de P et Q est le multiset où la multiplicité d'un élément est le minimum des multiplicités de P et Q . le **la différence** de P et Q est le multiset où la multiplicité d'un élément est la multiplicité de l'élément en P moins sa multiplicité dans Q, sauf si cette différence est négative, dans laquelle cas, la multiplicité est 0. La **somme** de P et Q est le multi-ensemble où la multiplicité d'un élément est la somme des multiplications ITIES en P et Q . L'union, l'intersection et la différence de P et Q sont désignés par $P \cup Q$, $P \cap Q$ et $P - Q$, respectivement (où ces opérations ne doivent pas être confondues avec les opérations analogues pour les ensembles). La somme de P et Q est désigné par $P + Q$.

61. Soit A et B les multisets $\{3 \cdot a, 2 \cdot b, 1 \cdot c\}$ et $\{2 \cdot a, 3 \cdot b, 4 \cdot d\}$, respectivement. Trouver

a) $A \cup B$. **b)** $A \cap B$. **c)** $A - B$.
d) $B - A$. **e)** $A + B$.

62. Supposons que A est le multiset qui a pour éléments les types d'équipements informatiques nécessaires à un d'une université et les multiplicités sont le nombre de pièces de chaque type nécessaires, et B est l'analogue multiset pour un deuxième département de l'université. Pour par exemple, A pourrait être le multiset $\{107 \cdot$ calcul personnel ers, $44 \cdot$ routeurs, $6 \cdot$ serveurs$\}$ et B pourraient être le multiset $\{14 \cdot$ ordinateurs personnels, $6 \cdot$ routeurs, $2 \cdot$ mainframes$\}$.

a) Quelle combinaison de A et B représente l'équipement l'université devrait acheter en supposant que les deux utilisent le même équipement?

b) Quelle combinaison de A et B représente l'équipement qui sera utilisé par les deux départements si les deux les ministères utilisent le même équipement?

c) Quelle combinaison de A et B représente l'équipement ment que le deuxième département utilise, mais le premier pas si les deux départements utilisent le même équipement?

d) Quelle combinaison de A et B représente l'équipement ment que l'université devrait acheter si le département ne partagent pas l'équipement?

Les ensembles flous sont utilisés en intelligence artificielle. Chaque élément dans l'ensemble universel U a un **degré d'appartenance** , qui est un nombre réel compris entre 0 et 1 (dont 0 et 1), dans un ensemble flou S . L'ensemble flou S est noté en listant les éléments avec leurs degrés d'appartenance (éléments avec 0 degré de les membres ne sont pas répertoriés). Par exemple, nous écrivons {0,6 Alice, 0,9 Brian, 0,4 Fred, 0,1 Oscar, 0,5 Rita} pour l'ensemble F (de fa- personnes) pour indiquer qu'Alice a un degré de mémoire de 0,6 bership en F , Brian a une adhésion de 0,9 degré en F , Fred a un degré d'appartenance à F *de* 0,4 , Oscar a un degré de 0,1 d'appartenance à F , et Rita a un degré d'adhésion de 0,5 en F (pour que Brian soit le plus célèbre et Oscar le moins célèbre de ces gens). Supposons également que R est l'ensemble des riches personnes avec R = {0,4 Alice, 0,8 Brian, 0,2 Fred, 0,9 Oscar, 0,7 Rita}.

63. Le **complément** d'un ensemble flou S est l'ensemble S , avec le degré d'appartenance d'un élément dans S égal à 1 moins le degré d'appartenance de cet élément dans S . Trouvez F (l'ensemble flou de personnes qui ne sont pas célèbres) et R (l'ensemble flou de personnes qui ne sont pas riches).

64. L' **union** de deux ensembles flous S et T est l'ensemble flou $S \cup T$, où le degré d'appartenance d'un élément dans $S \cup T$ est le maximum des degrés d'appartenance à cet élément en S et T . Trouver l'ensemble flou $F \cup R$ de des gens riches ou célèbres.

65. L' **intersection** de deux ensembles flous S et T est le flou définir $S \cap T$, où le degré d'appartenance d'un élément dans $S \cap T$ est le minimum des degrés d'appartenance de cet élément en S et T . Trouver l'ensemble flou $F \cap R$ de gens riches et célèbres.

Fonctions

introduction

Dans de nombreux cas, nous attribuons à chaque élément d'un ensemble un élément particulier d'un deuxième ensemble (qui peut être le même que le premier).Par exemple, supposons que chaque élève d'une mathématique discrète une classe est attribuée à la classe à partir de l'ensemble $\{A, B, C, D, F\}$. Et supposons que les notes soient A pour Adams, C pour Chou, B pour Goodfriend, A pour Rodriguez et F pour Stevens. Cette mission des notes est illustré à la figure 1.

Cette affectation est un exemple de fonction. Le concept de fonction est extrêmement important tant en mathématiques et en informatique. Par exemple, en mathématiques discrètes, les fonctions sont utilisé dans la définition de structures discrètes telles que des séquences et des chaînes. Les fonctions sont également utilisé pour représenter le temps qu'il faut à un ordinateur pour résoudre des problèmes d'une taille donnée. Beaucoup d'ordinateur les programmes et les sous-programmes sont conçus pour calculer les valeurs des fonctions. Fonctions récursives,

Adams	*UNE*
Chou	*B*
Bon ami	*C*
Rodriguez	*ré*
Stevens	*F*

FIGURE 1 **Affectation des notes dans une classe de mathématiques discrètes.**

qui sont des fonctions définies en soi, sont utilisées dans toute l'informatique; ils sera étudiée au chapitre 5. Cette section passe en revue les concepts de base impliquant les fonctions nécessaires en mathématiques discrètes.

DÉFINITION 1 Soit A et B *des* ensembles non vides. Une *fonction* f de A à B est une affectation d'exactement une Elément de B à chaque élément de A . On écrit $f(a) = b$ si b est l'élément unique de B attribué par la fonction f à l'élément *un* de A . Si f est une fonction de A à B , on écrit $f : A \rightarrow B$.

Remarque: Les fonctions sont parfois également appelées **mappages** ou **transformations** .

Les fonctions sont spécifiées de différentes manières. Parfois, nous déclarons explicitement comme dans la figure 1. Souvent, nous donnons une formule, telle que $f(x) = x + 1$, pour définir une fonction. D'autres fois, nous utilisons un programme informatique pour spécifier une fonction.

Une fonction $f : A \rightarrow B$ peut également être définie en termes d'un rapport de A à B . Rappel de Section 2.1 qu'une relation de A à B est juste un sous -ensemble de $A \times B$. Une relation de A à B qui contient une et une seule paire ordonnée (a, b) pour chaque élément $a \in A$, définit une fonction f de A à B . Cette fonction est définie par l'affectation $f(a) = b$, où (a, b) est l'unique paire ordonnée dans la relation qui a *un* comme premier élément.

DÉFINITION 2 Si f est une fonction de A à B , on dit que A est le *domaine* de f et B est le *codomaine* de *f*. Si $f(a) = b$, on dit que b est l' *image* de a et a est une *pré-image* de b . La *plage* , ou l' *image* , de f est l'ensemble de toutes les images des éléments de A . De plus, si f est une fonction de A à B , on dit que f *cartes* A à B .

La figure 2 représente une fonction f de A à B .

Lorsque nous définissons une fonction, nous spécifions son domaine, son domaine de codage et le mappage des éléments du domaine aux éléments du codomaine. Deux fonctions sont **égales** lorsqu'elles ont le même domaine, ont le même codomaine et mappent chaque élément de leur domaine commun sur le même élément de leur codomaine commun. Notez que si nous changeons le domaine ou le domaine de codage

F

une $b = f(a)$

UNE *F* *B*

FIGURE 2 **La fonction *f* cartes *A* à *B* .**

d'une fonction, alors nous obtenons une fonction différente. Si nous changeons la cartographie des éléments, alors nous obtenons également une fonction différente.

Les exemples 1 à 5 fournissent des exemples de fonctions. Dans chaque cas, nous décrivons le domaine, le codomaine, la plage et l'affectation de valeurs aux éléments du domaine.

EXEMPLE 1 Quels sont le domaine, le domaine codé et la plage de la fonction qui attribue les notes aux étudiants décrit dans le premier paragraphe de l'introduction de cette section?

Solution: Soit G la fonction qui attribue une note à un élève de notre classe de mathématiques discrètes. Notez que G (Adams) $= A$, par exemple. Le domaine de G est l'ensemble {Adams, Chou, Goodfriend, Rodriguez, Stevens} et le codomaine est l'ensemble $\{A, B, C, D, F\}$. La plage de G est l'ensemble $\{A, B, C, F\}$, car chaque note, à l'exception de D, est attribuée à un élève. ▲

EXEMPLE 2 Soit R la relation avec les paires ordonnées (Abdul, 22), (Brenda, 24), (Carla, 21), (Désir, 22), (Eddie, 24 ans) et (Felicia, 22 ans). Ici, chaque paire se compose d'un étudiant diplômé et de cet étudiant âge. Spécifiez une fonction déterminée par cette relation.

Solution: si f est une fonction spécifiée par R , alors f (Abdul) = 22, f (Brenda) = 24, f (Carla) = 21, f (Désir) = 22, f (Eddie) = 24, et f (Felicia) = 22. (Ici, $f(x)$ est l'âge de x , où x est un étudiant.) Pour le domaine, nous prenons l'ensemble {Abdul, Brenda, Carla, Desire, Eddie, Felicia}. Nous devons également spécifier un codomaine, qui doit contenir tous les âges possibles des étudiants. Comme il est très probable que tous les élèves aient moins de 100 ans, nous pouvons prendre l'ensemble des entiers positifs inférieurs à 100 comme codomaine. (Notez que nous pourrions choisir un autre codomaine, comme l'ensemble de tous les entiers positifs ou l'ensemble des entiers positifs compris entre 10 et 90, mais cela changerait la fonction. L'utilisation de ce codomaine nous permettra également d'étendre la fonction en ajoutant les noms et les âges de plus d'élèves plus tard.) La gamme de la fonction que nous ont spécifié est l'ensemble des âges différents de ces élèves, qui est l'ensemble $\{21, 22, 24\}$. ▲

EXEMPLE 3 Soit f la fonction qui affecte les deux derniers bits d'une chaîne de bits de longueur 2 ou supérieure à celle chaîne. Par exemple, $f(11010) = 10$. Ensuite, le domaine de f est l'ensemble de toutes les chaînes de bits de longueur 2 ou plus, et le domaine de codage et la plage sont l'ensemble $\{00, 01, 10, 11\}$. ▲

EXEMPLE 4 Soit $f : \mathbf{Z} \rightarrow \mathbf{Z}$ assigner le carré d'un entier à cet entier. Ensuite, $f(x) = x^2$, où le domaine de f est l'ensemble de tous les entiers, le domaine codé de f est l'ensemble de tous les entiers, et la plage de f est l'ensemble de tous les entiers qui sont des carrés parfaits, à savoir $\{0, 1, 4, 9, \ldots\}$. ▲

EXEMPLE 5 Le domaine et le domaine codé des fonctions sont souvent spécifiés dans les langages de programmationPour par exemple, l'instruction Java

int **floor** (float real) {... }

et l'instruction de fonction C ++

fonction int (float x) {... }

les deux nous disent que le domaine de la fonction de plancher est l'ensemble des nombres réels (représentés par nombres à virgule flottante) et son codomaine est l'ensemble des entiers. ▲

Une fonction est appelée valeur **réelle** si son codomaine est l'ensemble des nombres réels, et elle est appelée **valeur entière** si son codomaine est l'ensemble des entiers. Deux fonctions à valeur réelle ou deux entiers des fonctions de valeur avec le même domaine peuvent être ajoutées ou multipliées.

DÉFINITION 3 Soit f_1 et f_2 être des fonctions de A à **R**. Alors $f_1 + f_2$ et $f_1 f_2$ sont également des fonctions de A à **R** défini pour tout $x \in A$ par

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 f_2)(x) = f_1(x) f_2(x).$$

Notez que les fonctions $f_1 + f_2$ et $f_1 f_2$ ont été définies en spécifiant leurs valeurs à x dans termes des valeurs de f_1 et f_2 en x.

EXEMPLE 6 Soit f_1 et f_2 des fonctions de **R** à **R** telles que $f_1(x) = x^2$ et $f_2(x) = x - x^2$. Quels sont les fonctions $f_1 + f_2$ et $f_1 f_2$?

Solution: De la définition de la somme et du produit des fonctions, il s'ensuit que

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

et

$$(f_1 f_2)(x) = x^2 (x - x^2) = x^3 - x^4.$$ ▲

Lorsque f est une fonction de A à B, l'image d'un sous-ensemble de A peut également être définie.

DÉFINITION 4 Soit f une fonction de A à B et soit S un sous - ensemble de A. L' *image* de S sous la fonction f est le sous -ensemble de B constitué par les images des éléments de S. Nous désignons l'image de S par $f(S)$, donc

$$f(S) = \{ t \mid \exists s \in S \ (t = f(s)) \}.$$

Nous utilisons également le raccourci $\{f(s) \mid s \in S\}$ pour désigner cet ensemble.

Remarque: La notation $f(S)$ pour l'image de l'ensemble S sous la fonction f est potentiellement ambigu. Ici, $f(S)$ désigne un ensemble, et non la valeur de la fonction f pour l'ensemble S.

EXEMPLE 7 Soit $A = \{a, b, c, d, e\}$ et $B = \{1, 2, 3, 4\}$ avec $f(a) = 2$, $f(b) = 1$, $f(c) = 4$, $f(d) = 1$, et $f(e) = 1$. L'image du sous-ensemble $S = \{b, c, d\}$ est l'ensemble $f(S) = \{1, 4\}$. ▲

Fonctions un à un et sur

Certaines fonctions n'attribuent jamais la même valeur à deux éléments de domaine différents.Ces fonctions sont censés être **un à un**.

DÉFINITION 5 Une fonction f est dite *un à un,* ou une *injonction,* si et seulement si $f(a) = f(b)$ implique que $a = b$ pour tout a et b dans le domaine de f. Une fonction est dite *injective* si elle est *biunivoque*.

une 1

b 2

c 3

ré 4

5

FIGURE 3 **Une fonction un à un.**

Notez qu'une fonction f est *biunivoque* si et seulement si $f(a) = f(b)$ chaque fois *que* $a = b$. Par ici d'exprimer que f est un à un est obtenu en prenant la contrapositive de l'implication dans la définition.

Remarque: Nous pouvons exprimer que f est un à un en utilisant des quantificateurs comme $\forall a \forall b\ (f(a) = f(b) \rightarrow a = b)$ ou de manière équivalente $\forall a \forall b\ (a = b \rightarrow f(a) = f(b))$, où l'univers du discours est le domaine de la fonction.

Nous illustrons ce concept en donnant des exemples de fonctions individuelles et autres fonctions qui ne sont pas un à un.

EXEMPLE 8 Déterminer si la fonction f de $\{a, b, c, d\}$ à $\{1, 2, 3, 4, 5\}$ avec $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, et $f(d) = 3$ est un à un.

Solution: la fonction f est *biunivoque* car f prend des valeurs différentes aux quatre éléments de son domaine. Ceci est illustré à la figure 3. ▲

EXEMPLE 9 Déterminer si la fonction $f(x) = x^2$ de l'ensemble des entiers à l'ensemble des entiers est Un par un.

Solution: la fonction $f(x) = x^2$ n'est pas biunivoque car, par exemple, $f(1) = f(-1) = 1$, mais 1 = -1.

Notez que la fonction $f(x) = x^2$ avec son domaine limité à $\mathbf{Z}^+$ est un à un. (Techni-
En fait, quand on restreint le domaine d'une fonction, on obtient une nouvelle fonction dont les valeurs s'accordent avec ceux de la fonction d'origine pour les éléments du domaine restreint. Le restreint n'est pas définie pour les éléments du domaine d'origine en dehors du domaine restreint.) ▲

EXEMPLE 10 Déterminer si la fonction $f(x) = x + 1$ de l'ensemble des nombres réels à elle-même est de un à un.

Solution: La fonction $f(x) = x + 1$ est une fonction biunivoque. Pour le démontrer, notez que $x + 1 = y + 1$ lorsque $x = y$. ▲

EXEMPLE 11 Supposons que chaque travailleur d'un groupe d'employés se voit attribuer un travail à partir d'un ensemble de travaux, chacun devant être effectué par un seul travailleur. Dans cette situation, la fonction f qui affecte un travail à chaque travailleur est un à un. Pour voir cela, notez que si x et y sont deux travailleurs différents, alors $f(x) = f(y)$ car les deux travailleurs x et y doivent se voir attribuer des emplois différents. ▲

Nous donnons maintenant quelques conditions qui garantissent qu'une fonction est biunivoque.

une

b 1

c 2

ré 3

FIGURE 4 Une fonction Onto.

DÉFINITION 6 Une fonction f dont le domaine et le domaine de codage sont des sous-ensembles de l'ensemble des nombres réels est appelée *croissant* si $f(x) \leq f(y)$, et *strictement croissant* si $f(x) < f(y)$, chaque fois que $x < y$ et x et y sont dans le domaine de f. De même, f est appelé *décroissant* si $f(x) \geq f(y)$, et *strictement décroissant* si $f(x) > f(y)$, chaque fois que $x < y$ et x et y sont dans le domaine de f. (Le mot *strictement* dans cette définition indique une stricte inégalité.)

Remarque: Une fonction f augmente si $\forall x \forall y (x < y \rightarrow f(x) \leq f(y))$, strictement croissante si $\forall x \forall y (x < y \rightarrow f(x) < f(y))$, diminuant si $\forall x \forall y (x < y \rightarrow f(x) \geq f(y))$, et strictement dé-froissant si $\forall x \forall y (x < y \rightarrow f(x) > f(y))$, où l'univers du discours est le domaine de f.

À partir de ces définitions, il peut être montré (voir exercices 26 et 27) qu'une fonction qui est soit strictement augmenter soit strictement diminuer doit être un à un. Cependant, une fonction qui est augmenter, mais pas strictement augmenter, ou diminuer, mais pas strictement diminuer, n'est pas un à un.

Pour certaines fonctions, la plage et le domaine de codage sont égaux. Autrement dit, chaque membre du codomain est l'image d'un élément du domaine. Les fonctions avec cette propriété sont appelées **sur les** fonctions.

DÉFINITION 7 Une fonction f de A à B est appelée , ou une *surjection,* si et seulement si pour chaque élément $b \in B$ il y a un élément $a \in A$ avec $f(a) = b$. Une fonction f est appelée *surjectif* si elle est sur.

Remarque: Une fonction f est sur si $\forall y \exists x (f(x) = y)$, où le domaine pour x est le domaine de la fonction et le domaine pour y est le codomaine de la fonction.

Nous donnons maintenant des exemples de fonctions on et de fonctions qui ne le sont pas.

EXEMPLE 12 Soit f la fonction de $\{a, b, c, d\}$ à $\{1, 2, 3\}$ définie par $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, et $f(d) = 3$. Est-ce que f est une fonction sur?

Solution: les trois éléments du domaine de codage étant des images d'éléments du domaine, nous voir que f est sur. Ceci est illustré dans la figure 4. Notez que si le codomaine était $\{1, 2, 3, 4\}$, alors f ne serait pas activé. ▲

EXEMPLE 13 La fonction $f(x) = x^2$ est-elle de l'ensemble des entiers à l'ensemble des entiers sur?

Solution: La fonction f n'est pas activée car il n'y a pas d'entier x avec $x^2 = -1$, par exemple. ▲

EXEMPLE 14 La fonction $f(x) = x + 1$ est-elle de l'ensemble des entiers à l'ensemble des entiers sur?

(une) Un par un, pas sur | b) Sur, pas un à un | (c) Un par un, et sur | (ré) Ni en tête-à-tête ni sur | e) Pas une fonction

1 *une* *une* 1 *une* 1 1

une 1 *une*

2 *b* *b* 2 *b* 2 2

b 2 *b*

3 *c* *c* 3 *c* 3 3

c 3 *c*

4 *ré* *ré* 4 *ré* 4 4

FIGURE 5 Exemples de différents types de correspondances.

Solution: cette fonction est activée, car pour chaque entier y, il existe un entier x tel que $f(x) = y$. Pour voir cela, notons que $f(x) = y$ si et seulement si $x + 1 = y$, qui vaut si et seulement si $x = y - 1$. ▲

EXEMPLE 15 Considérons la fonction f de l'exemple 11 qui attribue des tâches aux travailleurs. La fonction f est sur if pour chaque emploi, un travailleur est affecté à cet emploi. La fonction f n'est pas activée lorsqu'il y a au moins un travail auquel aucun travailleur ne lui a été attribué. ▲

DÉFINITION 8 La fonction f est une *correspondance biunivoque,* ou une *bijection,* si elle est à la fois *biunivoque* et sur. Nous disons également qu'une telle fonction est *bijective* .

Les exemples 16 et 17 illustrent le concept de bijection.

EXEMPLE 16 Soit f la fonction de $\{a, b, c, d\}$ à $\{1, 2, 3, 4\}$ avec $f(a) = 4$, $f(b) = 2$, $f(c) = 1$, et $f(d) = 3$. Est-ce que f est une bijection?

Solution: La fonction f est un à un et sur. C'est un à un car il n'y a pas deux valeurs dans les mêmes valeurs de fonction sont attribuées au domaine. C'est parce que les quatre éléments du codomaine sont des images d'éléments du domaine. Par conséquent, f est une bijection. ▲

La figure 5 montre quatre fonctions où la première est un à un mais pas sur, la seconde est sur mais pas un à un, le troisième est à la fois un à un et sur, et le quatrième n'est ni un à un ni sur. La cinquième correspondance de la figure 5 n'est pas une fonction, car elle envoie un élément à deux éléments différents.

Supposons que f soit une fonction d'un ensemble A à lui-même. Si A est fini, alors f est un à un si et seulement si c'est sur. (Cela découle du résultat de l'exercice 72.) Ce n'est pas nécessairement le cas si A est infini (comme cela sera montré dans la section 2.5).

EXEMPLE 17 Soit A un ensemble. La *fonction d'identité* sur A est la fonction $\iota_A : A \rightarrow A$, où

$$\iota_A(x) = x$$

pour tout $x \in A$. En d'autres termes, la fonction d'identité ι_A est la fonction qui attribue chaque élément à lui-même. La fonction ι_A est un à un et sur, c'est donc une bijection. (Notez que ι est le grec lettre iota.) ▲

Pour référence future, nous résumons ce qui doit être montré pour établir si une fonction est un à un et si c'est le cas. Il est instructif de revoir les exemples 8 à 17 à la lumière de ce sommaire.

On suppose que $f : A \rightarrow B$.

Pour montrer que f est injective Montrez que si $f(x) = f(y)$ pour x arbitraire , $y \in A$ avec $x = y$, alors $x = y$.

Pour montrer que f n'est pas injectif Trouver des éléments particuliers $x, y \in A$ tels que $x = y$ et $f(x) = f(y)$.

Pour montrer que f est surjectif Considérons un élément arbitraire $y \in B$ et trouvons un élément $x \in A$ tel que $f(x) = y$.

Pour montrer que f est pas surjective Trouver un particulier $y \in B$ tel que $f(x) = y$ pour tout $x \in A$.

Fonctions inverses et compositions de fonctions

Considérons maintenant un one-to-one correspondance f de l'ensemble A à l'ensemble B . Parce que f est un sur fonction, chaque élément de B est l'image d'un élément dans A . De plus, parce que f est aussi un one-to-one fonction, chaque élément de B est l'image d'un *unique* , élément de A . Par conséquent, on peut définir une nouvelle fonction de B vers A qui inverse la correspondance donnée par f . Cette conduit à la définition 9.

DÉFINITION 9 Soit f soit un one-to-one correspondance de l'ensemble A à l'ensemble B . La *fonction inverse* de f est la fonction qui assigne à un élément b appartenant à B l'élément unique a dans A tel que $f(a) = b$. La fonction inverse de f est notée f^{-1} . Par conséquent, $f^{-1}(b) = a$ lorsque $f(a) = b$.

Remarque: veillez à ne pas confondre la fonction f^{-1} avec la fonction $1/f$, qui est la fonction qui attribue à chaque x du domaine la valeur $1/f(x)$. Notez que ce dernier n'a de sens que lorsque $f(x)$ est un nombre réel non nul.

La figure 6 illustre le concept d'une fonction inverse.

Si une fonction f n'est pas une correspondance biunivoque, on ne peut pas définir une fonction inverse de f . Lorsque f n'est pas une correspondance biunivoque, ce n'est pas une correspondance biunivoque ou ce n'est pas le cas.Si

f n'est pas un à un, un élément b dans le domaine codé est l'image de plusieurs éléments dans le domaine. Si f n'est pas sur, pour un élément b dans le domaine codé, aucun élément a dans le domaine existe pour lequel $f(a) = b$. Par conséquent, si f n'est pas une correspondance biunivoque, nous ne pouvons pas affecter à chaque élément b du domaine de codage un élément unique a dans le domaine tel que $f(a) = b$ (parce que pour certains b il est soit plus d'un tel *un* ou une telle a).

Une correspondance biunivoque est appelée **inversible** parce que nous pouvons définir un inverse de cette une fonction. Une fonction n'est **pas inversible** si ce n'est pas une correspondance biunivoque, car le l'inverse d'une telle fonction n'existe pas.

$f^{-1}(b)$

$a = f^{-1}(b)$ $f(a)$ $b = f(a)$

f^{-1}

UNE *B*

F

FIGURE 6 La fonction f^{-1} Est l'inverse de la fonction f .

EXEMPLE 18 Soit f la fonction de $\{a, b, c\}$ à $\{1, 2, 3\}$ telle que $f(a) = 2$, $f(b) = 3$ et $f(c) = 1$. F est-il inversible, et si tel est le cas, quel est son inverse?

Solution: La fonction f est inversible car il s'agit d'une correspondance biunivoque. L'in- fonction verset f^{-1} inverse la correspondance donnée par f , donc $f^{-1}(1) = c$, $f^{-1}(2) = a$, et $f^{-1}(3) = b$. ▲

EXEMPLE 19 Soit $f : \mathbf{Z} \to \mathbf{Z}$ tel que $f(x) = x + 1$. Est-ce que f est inversible, et si c'est le cas, quelle est son inverse?

Solution: la fonction f a un inverse car il s'agit d'une correspondance biunivoque, comme suit des exemples 10 et 14. Pour inverser la correspondance, supposons que y est l'image de x , donc que $y = x + 1$. Alors $x = y - 1$. Cela signifie que $y - 1$ est l'élément unique de $\mathbf{Z}$ qui est envoyé à y par f . Par conséquent, $f^{-1}(y) = y - 1$. ▲

EXEMPLE 20 Soit f la fonction de $\mathbf{R}$ à $\mathbf{R}$ avec $f(x) = x^2$. Est-ce que f est inversible?

Solution: parce que $f(-2) = f(2) = 4$, f n'est pas un à un. Si une fonction inverse était définie, il faudrait affecter deux éléments à 4. Par conséquent, f n'est pas inversible. (Notez que nous pouvons également montrer que f n'est pas inversible car il n'est pas sur.) ▲

Parfois, nous pouvons restreindre le domaine ou le domaine codé d'une fonction, ou les deux, pour obtenir un fonction inversible, comme l'illustre l'exemple 21.

EXEMPLE 21 Montrer que si l'on restreint la fonction $f(x) = x^2$ dans l'exemple 20 à une fonction de l'ensemble de tous nombres réels non négatifs à l'ensemble de tous les nombres réels non négatifs, alors f est inversible.

Solution: La fonction $f(x) = x^2$ de l'ensemble des nombres réels non négatifs à l'ensemble des non les nombres réels négatifs sont un à un. Pour voir cela, notez que si $f(x) = f(y)$, alors $x^2 = y^2$, donc $x^2 - y^2 = (x + y)(x - y) = 0$. Cela signifie que $x + y = 0$ ou $x - y = 0$, donc $x = -y$ ou $x = y$.

Parce que x et y sont non négatifs, nous devons avoir $x = y$. Donc, cette fonction est biunivoque. De plus, $f(x) = x^2$ est sur lorsque le codomaine est l'ensemble de tous les nombres réels non négatifs, parce que chaque nombre réel non négatif a une racine carrée. Autrement dit, si y est un réel non négatif nombre, il existe un nombre réel non négatif x tel que $x = \sqrt{y}$, ce qui signifie que $x^2 = y$.

Parce que la fonction $f(x) = x^2$ de l'ensemble des nombres réels non négatifs à l'ensemble des non les nombres réels négatifs sont un à un et sur, ils sont inversibles. Son inverse est donné par la règle $f^{-1}(y) = \sqrt{y}$. ▲

DÉFINITION 10 Soit g une fonction de l'ensemble A à l'ensemble B et f une fonction de l'ensemble B à la Série C . La *composition* des fonctions f et g , notée pour tout $a \in A$ par $f \circ g$, est définie par

$$(f \circ g)(a) = f(g(a)).$$

En d'autres termes, $f \circ g$ est la fonction qui assigne à l'élément a de A l'élément assigné par f à $g(a)$. Autrement dit, pour trouver $(f \circ g)(a)$, nous appliquons d'abord la fonction g à a pour obtenir $g(a)$ et on applique ensuite la fonction f au résultat $g(a)$ pour obtenir $(f \circ g)(a) = f(g(a))$. Notez que le la composition $f \circ g$ ne peut être définie que si la plage de g est un sous-ensemble du domaine de f. Dans La figure 7 montre la composition des fonctions.

$(f \quad g)(a)$

$g(a)$ $f(g(a))$

une $g(a)$ $f(g(a))$

g *F*

UNE *B* *C*

fg

FIGURE 7 La composition des fonctions *f* et *g* .

EXEMPLE 22 Soit g la fonction de l'ensemble $\{a, b, c\}$ à lui-même telle que $g(a) = b$, $g(b) = c$, et $g(c) = a$. Soit f la fonction de l'ensemble $\{a, b, c\}$ à l'ensemble $\{1, 2, 3\}$ telle que $f(a) = 3$, $f(b) = 2$, et $f(c) = 1$. Quelle est la composition de f et g, et quelle est la composition de g et f ?

Solution: La composition $f \circ g$ est définie par $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, et $(f \circ g)(c) = f(g(c)) = f(a) = 3$.

Notez que $g \circ f$ n'est pas défini, car la plage de f n'est pas un sous-ensemble du domaine de g. ▲

EXEMPLE 23 Soit f et g les fonctions de l'ensemble des entiers à l'ensemble des entiers définis par $f(x) = 2x + 3$ et $g(x) = 3x + 2$. Quelle est la composition de f et g ? Quelle est la position de g et f ?

Solution: Les compositions $f \circ g$ et $g \circ f$ sont définies. En outre,

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

et

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$

▲

Remarque: Notez que même si $f \circ g$ et $g \circ f$ sont définis pour les fonctions f et g dans Exemple 23, $f \circ g$ et $g \circ f$ ne sont pas égaux. En d'autres termes, la loi commutative ne tient pas pour la composition des fonctions.

Lorsque la composition d'une fonction et son inverse est formée, dans l'un ou l'autre ordre, une identité est obtenue. Pour voir cela, supposons que f est une correspondance biunivoque de l'ensemble A à l'ensemble B. Alors la fonction inverse f^{-1} existe et est une correspondance biunivoque de B à A. La fonction inverse inverse la correspondance de la fonction d'origine, donc $f^{-1}(b) = a$ lorsque $f(a) = b$, et $f(a) = b$ lorsque $f^{-1}(b) = a$. Par conséquent,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a,$$

et

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b.$$

Par conséquent $f^{-1} \circ f = \iota_A$ et $f \circ f^{-1} = \iota_B$, où ι_A et ι_B sont les fonctions identitaires sur les ensembles A et B, respectivement. Autrement dit, $(f^{-1})^{-1} = f$.

Les graphiques des fonctions

On peut lui associer un ensemble de paires de $A \times B$ pour chaque fonction de A à B . Cet ensemble de paires est appelé le **graphique** de la fonction et est souvent affiché sous forme d'image pour aider à comprendre le comportement de la fonction.

DÉFINITION 11 Soit f une fonction de l'ensemble A à l'ensemble B . Le *graphe* de la fonction f est l'ensemble des paires ordonnées $\{(a, b) \mid a \in A$ et $f(a) = b\}$.

D'après la définition, le graphe d'une fonction f de A à B est le sous-ensemble de $A \times B$ contenant le paires ordonnées avec la deuxième entrée égale à l'élément de B attribué par f à la première entrée. Notez également que le graphique d'une fonction f de A à B est le même que la relation de A à B déterminé par la fonction f , comme décrit à la page 139.

EXEMPLE 24 Afficher le graphique de la fonction $f(n) = 2n + 1$ de l'ensemble des entiers à l'ensemble des entiers.

Solution: Le graphe de f est l'ensemble des paires ordonnées de la forme $(n, 2n + 1)$, où n est un entier. Ce graphique est illustré à la figure 8. ▲

EXEMPLE 25 Affichez le graphique de la fonction $f(x) = x^2$ de l'ensemble des entiers à l'ensemble des entiers.

Solution: Le graphique de f est l'ensemble des paires ordonnées de la forme $(x, f(x)) = (x, x^2)$, où x est un nombre entier. Ce graphique est illustré à la figure 9. ▲

Quelques fonctions importantes

Ensuite, nous introduisons deux fonctions importantes en mathématiques discrètes, à savoir le sol et le plafond les fonctions. Soit x un nombre réel. La fonction de plancher arrondit x vers le bas à l'entier le plus proche moins supérieur ou égal à x , et la fonction de plafond arrondit x à l'entier le plus proche supérieur ou égal à x . Ces fonctions sont souvent utilisées lorsque les objets sont comptés. Ils jouent un rôle important rôle dans l'analyse du nombre d'étapes utilisées par les procédures pour résoudre les problèmes d'un Taille.

(–3,9) (3,9)

(–2,4) (2,4)

(–1,1) (1,1)

(0,0)

FIGURE 8 Le graphique de $f(n) = 2n + 1$ de Z à Z.

FIGURE 9 Le graphique de $f(x) = x^2$ de Z à Z.

DÉFINITION 12 La *fonction de plancher* attribue au nombre réel x le plus grand entier inférieur ou égal à x . La valeur de la fonction de plancher à x est notée $\lfloor x \rfloor$. La *fonction plafond* attribue au nombre réel x le plus petit entier supérieur ou égal à x . La valeur du plafond la fonction en x est notée $\lceil x \rceil$.

Remarque: La fonction floor est souvent aussi appelée la *plus grande fonction entière* . Il est souvent noté par $[x]$.

EXEMPLE 26 Voici quelques valeurs des fonctions de plancher et de plafond:

$$\lfloor \tfrac{1}{2} \rfloor = 0, \lceil \tfrac{1}{2} \rceil = 1, \lfloor -\tfrac{1}{2} \rfloor = -1, \lceil -\tfrac{1}{2} \rceil = 0, \lfloor 3.1 \rfloor = 3, \lceil 3.1 \rceil = 4, \lfloor 7 \rfloor = 7, \lceil 7 \rceil = 7.$$ ▲

Nous affichons les graphiques des fonctions de plancher et de plafond dans la figure 10. Dans la figure 10 (a), nous affichons le graphique de la fonction plancher $\lfloor x \rfloor$. Notez que cette fonction a la même valeur tout au long de la intervalle $[n, n + 1)$, à savoir n , puis il passe à $n + 1$ lorsque $x = n + 1$. Dans la figure 10 (b) nous affichons le graphique de la fonction plafond $\lceil x \rceil$. Notez que cette fonction a la même valeur tout au long de l'intervalle $(n, n + 1]$, à savoir $n + 1$, puis saute à $n + 2$ lorsque x est un peu supérieur à $n + 1$.

Les fonctions de plancher et de plafond sont utiles dans une grande variété d'applications, y compris celles impliquant le stockage et la transmission de données.Considérez les exemples 27 et 28, typiques de base calculs effectués lors de l'étude des problèmes de communication de bases de données et de données.

EXEMPLE 27 Les données stockées sur un disque d'ordinateur ou transmises sur un réseau de données sont généralement représentées chaîne d'octets. Chaque octet est composé de 8 bits. Combien d'octets sont nécessaires pour coder 100 bits de données?

Solution: pour déterminer le nombre d'octets nécessaires, nous déterminons le plus petit entier à au moins aussi grand que le quotient lorsque 100 est divisé par 8, le nombre de bits dans un octet.Par conséquent, $\lceil 100 / 8 \rceil = \lceil 12.5 \rceil = 13$ octets sont requis. ▲

EXEMPLE 28 En mode de transfert asynchrone (ATM) (protocole de communication utilisé sur les réseaux dorsaux), les données sont organisées en cellules de 53 octets. Combien de cellules ATM peuvent être transmises en 1 minute sur une connexion qui transmet des données au taux de 500 kilobits par seconde?

Solution: en 1 minute, cette connexion peut transmettre $500, 000 \cdot 60 = 30, 000, 000$ bits. Chaque ATM la cellule fait 53 octets de long, ce qui signifie qu'elle fait $53 \cdot 8 = 424$ bits de long Pour déterminer le nombre

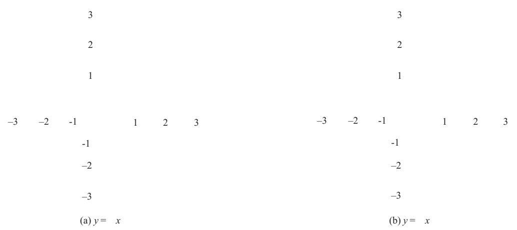


FIGURE 10 **Graphiques des fonctions (a) plancher et (b) plafond.**

TABLEAU 1 Propriétés utiles du sol et fonctions de plafond.
(n est un entier, x est un nombre réel)

(1a) $\lfloor x \rfloor = n$ si et seulement si $n \le x < n + 1$
(1b) $\lceil x \rceil = n$ si et seulement si $n - 1 < x \le n$
(1c) $\lfloor x \rfloor = n$ si et seulement si $x - 1 < n \le x$
(1d) $\lceil x \rceil = n$ si et seulement si $x \le n < x + 1$

(2) $x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$

(3a) $\lfloor -x \rfloor = -\lceil x \rceil$
(3b) $\lceil -x \rceil = -\lfloor x \rfloor$

(4a) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$
(4b) $\lceil x + n \rceil = \lceil x \rceil + n$

de cellules qui peuvent être transmises en 1 minute, nous déterminons le plus grand entier ne dépassant pas la quotient lorsque 30 , 000 , 000 est divisé par 424. Par conséquent, 00030 , 000 , 000 / 424⌋ = 70 , 754 ATM les cellules peuvent être transmises en 1 minute sur une connexion de 500 kilobits par seconde. ▲

Le tableau 1, avec x désignant un nombre réel, affiche certaines propriétés simples mais importantes du fonctions de plancher et de plafond. Parce que ces fonctions apparaissent si fréquemment en mathématiques discrètes, il est utile de regarder ces identités. Chaque propriété de ce tableau peut être établie à l'aide de la propriété définitions des fonctions de plancher et de plafond. Les propriétés (1a), (1b), (1c) et (1d) suivent directement à partir de ces définitions. Par exemple, (1a) indique que $\lfloor x \rfloor = n$ si et seulement si l'entier n est inférieur supérieur ou égal à x et $n + 1$ est supérieur à x . C'est précisément ce que signifie pour n être le plus grand entier ne dépassant pas x , qui est la définition de $\lfloor x \rfloor = n$. Propriétés (1b), (1c) et (1d) peut être établi de la même manière. Nous prouverons la propriété (4a) en utilisant une preuve directe.

Preuve: Supposons que $\lfloor x \rfloor = m$, où m est un entier positif. Par propriété (1a), il s'ensuit que $m \le x < m + 1$. L'ajout de n aux trois quantités de cette chaîne de deux inégalités montre que $m + n \le x + n < m + n + 1$. En utilisant à nouveau la propriété (1a), nous voyons que $\lfloor x + n \rfloor = m + n = \lfloor x \rfloor + n$. Ceci complète la preuve. Les preuves des autres propriétés sont laissées en exercice.

Les fonctions de plancher et de plafond bénéficient de nombreuses autres propriétés utiles en plus de celles Tableau 1. Il existe également de nombreuses instructions sur ces fonctions qui peuvent sembler correctes, mais ne le sont pas. Nous considérerons les déclarations sur les fonctions de plancher et de plafond dans les exemples 29 et 30.

Une approche utile pour considérer les déclarations sur la fonction de plancher est de laisser $x = n + \epsilon$, où $n = \lfloor x \rfloor$ est un entier et ϵ , la partie fractionnaire de x , satisfait l'inégalité $0 \le \epsilon < 1$. De même, lorsque l'on considère des déclarations sur la fonction plafond, il est utile d'écrire $x = n - \epsilon$, où $n = \lceil x \rceil$ est un entier et $0 \le \epsilon < 1$.

EXEMPLE 29 Démontrer que si x est un nombre réel, alors $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Solution: Pour prouver cette affirmation, on laisse $x = n + \epsilon$, où n est un entier et $0 \le \epsilon < 1$. Il sont deux cas à considérer, selon que ϵ est inférieur ou supérieur ou égal à $\frac{1}{2}$. (La raison pour laquelle nous choisissons ces deux cas sera clairement indiquée dans la preuve.)

Nous considérons d'abord le cas où $0 \le \epsilon < \frac{1}{2}$. Dans ce cas, $2x = 2n + 2\epsilon$ et $\lfloor 2x \rfloor = 2n$ car $0 \le 2\epsilon < 1$. De même, $x + \frac{1}{2} = n + (\frac{1}{2} + \epsilon)$, donc $\lfloor x + \frac{1}{2} \rfloor = n$, car $0 < \frac{1}{2} + \epsilon < 1$.

Par conséquent, $\lfloor 2x \rfloor = 2n$ et $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + n = 2n$.

Ensuite, nous considérons le cas lorsque $\frac{1}{2} \leq \epsilon < 1$. Dans ce cas, $2x = 2n + 2\epsilon = (2n+1) + (2\epsilon - 1)$. Parce que $0 \leq 2\epsilon - 1 < 1$, il s'ensuit que $\lfloor 2x \rfloor = 2n + 1$. Parce que $\lfloor x + \frac{1}{2} \rfloor = \lfloor n + (\frac{1}{2} + \epsilon) \rfloor = \lfloor n + 1 + (\epsilon - \frac{1}{2}) \rfloor$ et $0 \leq \epsilon - \frac{1}{2} < 1$, il s'ensuit que $\lfloor x + \frac{1}{2} \rfloor = n + 1$. Par conséquent, $\lfloor 2x \rfloor = 2n + 1$ et $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = n + (n+1) = 2n + 1$. Cette confirme la preuve. ▲

EXEMPLE 30 Prouver ou infirmer que $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ pour tous les nombres réels x et y.

Solution: bien que cette déclaration puisse sembler raisonnable, elle est fausse. Un contre-exemple est appliqué par $x = \frac{1}{2}$ et $y = \frac{1}{2}$. Avec ces valeurs, nous constatons que $\lceil x + y \rceil = \lceil \frac{1}{2} + \frac{1}{2} \rceil = \lceil 1 \rceil = 1$, mais $\lceil x \rceil + \lceil y \rceil = \lceil \frac{1}{2} \rceil + \lceil \frac{1}{2} \rceil = 1 + 1 = 2$. ▲

Il existe certains types de fonctions qui seront utilisées tout au long du texte. Ceux-ci inclus fonctions polynomiales, logarithmiques et exponentielles. Un bref aperçu des propriétés de ces Les fonctions nécessaires dans ce texte sont données dans l'annexe 2. Dans ce livre, le journal de notation x sera utilisé pour désigner le logarithme à la base 2 de x, car 2 est la base que nous utiliserons habituellement pour logarithmes. On notera les logarithmes de la base b, où b est tout nombre réel supérieur à 1, par $\log_b x$, et le logarithme naturel par $\ln x$.

Une autre fonction que nous utiliserons tout au long de ce texte est la **fonction factorielle** $f : \mathbf{N} \to \mathbf{Z}^+$, notée $f(n) = n!$. La valeur de $f(n) = n!$ est le produit des n premiers entiers positifs, donc $f(n) = 1 \cdot 2 \cdots (n-1) \cdot n$ [et $f(0) = 0! = 1$].

EXEMPLE 31 On a $f(1) = 1! = 1$, $f(2) = 2! = 1 \cdot 2 = 2$, $f(6) = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$, et $f(20) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18 \cdot 19 \cdot 20 =$ 2.432.902.008.176.640.000. ▲

L'exemple 31 montre que la fonction factorielle croît extrêmement rapidement à mesure que n croît. La croissance rapide de la fonction factorielle est rendue plus claire par la formule de Stirling, résultat de mathématiques supérieures qui nous disent que $n! \sim \sqrt{2\pi n}\,(n/e)^n$. Ici, nous avons utilisé la notation $f(n) \sim g(n)$, ce qui signifie que le rapport $f(n)/g(n)$ approche 1 lorsque n croît sans limite (c'est-à-dire, $\lim_{n\to\infty} f(n)/g(n) = 1$). Le symbole $\sim$ est lu «est asymptotique à». La formule de Stirling est nommée après James Stirling, un mathématicien écossais du XVIIIe siècle.

JAMES STIRLING (1692-1770) James Stirling est né près de la ville de Stirling, en Écosse. Sa famille a fortement soutenu la Cause jacobite des Stuarts comme alternative à la couronne britannique. La première information connue sur James est qu'il est entré dans Balliol College, Oxford, sur une bourse en 1711. Cependant, il a perdu plus tard sa bourse quand il a refusé de prêter allégeance à la Couronne britannique. La première rébellion jacobéenne a eu lieu en 1715 et Stirling a été accusé de communiquer avec les rebelles. Il était accusé d'avoir maudit le roi George, mais il a été acquitté de ces accusations. Même s'il ne pouvait pas être diplômé d'Oxford car de sa politique, il y est resté plusieurs années. Stirling a publié son premier travail, qui a prolongé le travail de Newton sur les courbes planes, en 1717. Il se rend à Venise, où une chaire de mathématiques lui a été promise, rendez-vous malheureusement par. Néanmoins, Stirling est resté à Venise, poursuivant son travail mathématique. Il a fréquenté l'Université de Padoue en 1721, et en 1722, il est retourné à Glasgow. Stirling a apparemment fui l'Italie après avoir appris les secrets de l'industrie du verre italienne, évitant efforts des verriers italiens pour l'assassiner afin de protéger leurs secrets.

À la fin de 1724, Stirling s'installe à Londres, y restant 10 ans à enseigner les mathématiques et à s'engager activement dans la recherche. En 1730 il a publié *Methodus Differentialis*, son travail le plus important, présentant des résultats sur des séries infinies, des sommations, l'interpolation et quadrature. C'est dans ce livre que sa formule asymptotique pour $n!$ apparaît. Stirling a également travaillé sur la gravitation et la forme du Terre; il a déclaré, mais n'a pas prouvé, que la terre est un sphéroïde oblat. Stirling est retourné en Écosse en 1735, quand il a été nommé directeur d'une société minière écossaise. Il a très bien réussi dans ce rôle et a même publié un article sur la ventilation du mien arbres. Il a poursuivi ses recherches mathématiques, mais à un rythme réduit, pendant ses années dans l'industrie minière. Stirling est également noté pour arpenter la rivière Clyde dans le but de créer une série d'écluses pour la rendre navigable. En 1752, les citoyens de Glasgow lui a offert une bouilloire en argent pour récompenser ce travail.

Fonctions partielles

Un programme conçu pour évaluer une fonction peut ne pas produire la valeur correcte de la fonction pour tous les éléments du domaine de cette fonction. Par exemple, un programme peut ne pas produire un car l'évaluation de la fonction peut entraîner une boucle infinie ou un débordement. De même, dans mathématiques abstraites, nous voulons souvent discuter de fonctions qui ne sont définies que pour un sous-ensemble de les nombres réels, tels que $1/x$, $\sqrt{x}$ et $\arcsin(x)$. Nous pouvons également vouloir utiliser des notions telles que la fonction «plus jeune enfant», qui n'est pas définie pour un couple sans enfant, ou la «durée du lever du soleil », qui n'est pas défini pendant quelques jours au-dessus du cercle polaire arctique. Pour étudier de telles situations, nous utilisons le concept d'une fonction partielle.

DÉFINITION 13 Une *fonction partielle* f d'un ensemble A à un ensemble B est une affectation à chaque élément a d'un sous-ensemble de A, appelé le *domaine de définition* de f, d'un unique élément b dans B. Les ensembles A et B sont appelés respectivement *domaine* et *codomaine* de f. On dit que f n'est *pas défini* pour les éléments en A qui ne sont pas dans le domaine de définition de f. Lorsque le domaine de définition de f est égal A, on dit que f est une *fonction totale.*

Remarque: On écrit $f : A \to B$ pour indiquer que f est une fonction partielle de A à B. Notez que il s'agit de la même notation que celle utilisée pour les fonctions. Le contexte dans lequel la notation est utilisée détermine si f est une fonction partielle ou une fonction totale.

EXEMPLE 32 La fonction $f : \mathbf{Z} \to \mathbf{R}$ où $f(n) = \sqrt{n}$ est une fonction partielle de **Z** à **R** où le domaine de la définition est l'ensemble des entiers non négatifs. Notez que f n'est pas défini pour les entiers négatifs. ▲

Des exercices

1. Pourquoi f n'est-il pas une fonction de **R** à **R** si

a) $f(x) = 1/x$?
b) $f(x) = \sqrt{x}$?
c) $f(x) = \pm\sqrt{(x^2 + 1)}$?

2. Déterminez si f est une fonction de **Z** à **R** si

a) $f(n) = \pm n$.
b) $f(n) = \sqrt{n^2 + 1}$.
c) $f(n) = 1/(n^2 - 4)$.

3. Déterminer si f est une fonction de l'ensemble de tous les bits chaînes à l'ensemble des entiers si

a) $f(S)$ est la position d'un bit 0 dans S.
b) $f(S)$ est le nombre de bits à 1 dans S.
c) $f(S)$ est le plus petit entier i tel que le i ème bit de S est 1 et $f(S) = 0$ lorsque S est la chaîne vide, le chaîne sans bits.

4. Recherchez le domaine et la plage de ces fonctions. Notez que dans chaque cas, pour trouver le domaine, déterminez l'ensemble de éléments affectés de valeurs par la fonction.

a) la fonction qui attribue à chaque entier non négatif son dernier chiffre
b) la fonction qui attribue le prochain plus grand entier à un entier positif
c) la fonction qui attribue à une chaîne de bits le nombre de un bit dans la chaîne
d) la fonction qui attribue à une chaîne de bits le nombre de bits dans la chaîne

5. Recherchez le domaine et la plage de ces fonctions. Notez que dans chaque cas, pour trouver le domaine, déterminez l'ensemble de éléments affectés de valeurs par la fonction.

a) la fonction qui attribue à chaque chaîne de bits le numéro de ceux de la chaîne moins le nombre de zéros dans le chaîne
b) la fonction qui attribue à chaque chaîne de bits deux fois la nombre de zéros dans cette chaîne
c) la fonction qui attribue le nombre de bits restants lorsqu'une chaîne de bits est divisée en octets (qui sont des blocs de 8 bits)
d) la fonction qui attribue à chaque entier positif la le plus grand carré parfait ne dépassant pas cet entier

6. Recherchez le domaine et la plage de ces fonctions.

a) la fonction qui attribue à chaque paire d'intégrations positives gers le premier entier de la paire
b) la fonction qui attribue à chaque entier positif son plus grand chiffre décimal
c) la fonction qui attribue à une chaîne de bits le nombre de ceux moins le nombre de zéros dans la chaîne
d) la fonction qui attribue à chaque entier positif la le plus grand entier ne dépassant pas la racine carrée de la entier
e) la fonction qui affecte le plus longtemps à une chaîne de bits chaîne de ceux de la chaîne

7. Recherchez le domaine et la plage de ces fonctions.

a) la fonction qui attribue à chaque paire d'intégrations positives gers le maximum de ces deux entiers
b) la fonction qui attribue à chaque entier positif la nombre des chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 qui font ne pas apparaître sous la forme de chiffres décimaux de l'entier
c) la fonction qui attribue à une chaîne de bits le nombre de fois le bloc 11 apparaît
d) la fonction qui attribue à une chaîne de bits la valeur numérique position du premier 1 dans la chaîne et qui affecte la valeur 0 à une chaîne de bits composée de tous les 0

8. Recherchez ces valeurs.

a) $\lfloor 1.1 \rfloor$ **b)** $\lceil 1.1 \rceil$
c) $\lfloor -0.1 \rfloor$ **d)** $\lceil -0.1 \rceil$
e) $\lceil 2.99 \rceil$ **f)** $\lceil -2.99 \rceil$
g) $\lfloor \frac{1}{2} + \lceil \frac{1}{2} \rceil \rfloor$ **h)** $\lceil \lfloor \frac{1}{2} \rfloor + \lceil \frac{1}{2} \rceil + \frac{1}{2} \rceil$

9. Recherchez ces valeurs.

a) $\lceil \frac{3}{4} \rceil$ **b)** $\lfloor \frac{7}{8} \rfloor$
c) $\lceil -\frac{3}{4} \rceil$ **d)** $\lfloor -\frac{7}{8} \rfloor$
e) $\lceil 3 \rceil$ **f)** $\lfloor -1 \rfloor$
g) $\lfloor \frac{1}{2} + \lceil \frac{3}{2} \rceil \rfloor$ **h)** $\lfloor \frac{1}{2} \cdot \lfloor \frac{5}{2} \rfloor \rfloor$

10. Déterminez si chacune de ces fonctions à partir de $\{a, b, c, d\}$ en soi est un à un.

a) $f(a) = b, f(b) = a, f(c) = c, f(d) = d$
b) $f(a) = b, f(b) = b, f(c) = d, f(d) = c$
c) $f(a) = d, f(b) = b, f(c) = c, f(d) = d$

11. Quelles sont les fonctions de l'exercice 10?

12. Déterminez si chacune de ces fonctions de **Z** à **Z** est un à un.

a) $f(n) = n - 1$ **b)** $f(n) = n^2 + 1$
c) $f(n) = n^3$ **d)** $f(n) = \lceil n/2 \rceil$

13. Quelles sont les fonctions de l'exercice 12?

14. Déterminez si $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ est sur if

a) bureau.
b) bus assigné au chaperon dans un groupe de bus prenant étudiants en excursion.
c) salaire.
d) numéro de sécurité sociale.

18. Spécifiez un domaine de codage pour chacune des fonctions de l'exercice 16. Dans quelles conditions chacune de ces fonctions est-elle le domaine de codage sur lequel vous avez spécifié?

19. Spécifiez un domaine de codage pour chacune des fonctions de l'exercice 17. Dans quelles conditions chacune des fonctions est-elle le domaine de codage sur lequel vous avez spécifié?

20. Donnez un exemple de fonction de **N** à **N** qui est

a) un à un mais pas sur.
b) sur mais pas en tête-à-tête.
c) à la fois sur et un à un (mais différent de l'identification fonction communautaire).
d) ni en tête-à-tête ni sur.

21. Donnez une formule explicite pour une fonction de l'ensemble de entiers à l'ensemble des entiers positifs qui est

a) un à un, mais pas sur.
b) sur, mais pas en tête-à-tête.
c) un à un et sur.
d) ni en tête-à-tête ni sur.

22. Déterminer si chacune de ces fonctions est une bijection à partir de **R** à **R**.

a) $f(x) = -3x + 4$
b) $f(x) = -3x^2 + 7$
c) $f(x) = (x + 1)/(x + 2)$
d) $f(x) = x^5 + 1$

23. Déterminez si chacune de ces fonctions est une bijection à partir de **R** à **R**.

a) $f(m, n) = 2m - n$.
b) $f(m, n) = m^2 - n^2$.
c) $f(m, n) = m + n + 1$.
d) $f(m, n) = |m| - |n|$.
e) $f(m, n) = m^2 - 4$.

15. Déterminez si la fonction $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ est sur si

a) $f(m, n) = m + n$.
b) $f(m, n) = m^2 + n^2$.
c) $f(m, n) = m$.
d) $f(m, n) = |n|$.
e) $f(m, n) = m - n$.

16. Considérez ces fonctions parmi l'ensemble des élèves dans un cours de mathématiques discrètes. Dans quelles conditions le fonctionner en tête-à-tête s'il attribue à un étudiant son

a) numéro de téléphone portable.
b) numéro d'identification de l'étudiant.
c) note finale dans la classe.
d) ville natale.

17. Considérez ces fonctions parmi l'ensemble des enseignants dans un école. Dans quelles conditions la fonction est-elle individuelle s'il attribue à un enseignant son

a) $f(x) = 2x + 1$
b) $f(x) = x^2 + 1$
c) $f(x) = x^3$
d) $f(x) = (x^2 + 1) / (x^2 + 2)$

24. Soit $f : \mathbf{R} \to \mathbf{R}$ et laisser $f(x) > 0$ pour tout $x \in \mathbf{R}$. Spectacle que $f(x)$ augmente strictement si et seulement si la fonction tion $g(x) = 1 / f(x)$ est strictement décroissante.

25. Soit $f : \mathbf{R} \to \mathbf{R}$ et laisser $f(x) > 0$ pour tout $x \in \mathbf{R}$. Spectacle que $f(x)$ diminue strictement si et seulement si la fonction tion $g(x) = 1 / f(x)$ est strictement croissante.

26. a) Démontrer qu'une fonction strictement croissante de **R** à it-soi est un à un.

b) Donner un exemple de fonction croissante de **R** à lui-même qui n'est pas un à un.

27. a) Démontrer qu'une fonction strictement décroissante de **R** à lui-même est un à un.

b) Donnez un exemple de fonction décroissante de **R** à lui-même qui n'est pas un à un.

28. Montrer que la fonction $f(x) = e^x$ de l'ensemble du réel nombres à l'ensemble des nombres réels n'est pas inversible, mais si le codomaine est limité à l'ensemble des réels positifs nombres, la fonction résultante est inversible.

29. Montrer que la fonction $f(x) = |x|$ de l'ensemble du réel nombres à l'ensemble des nombres réels non négatifs n'est pas inversible, mais si le domaine est limité à l'ensemble des non nombres réels négatifs, la fonction résultante est inversible.

30. Soit $S = \{-1, 0, 2, 4, 7\}$. Trouvez $f(S)$ si

a) $f(x) = 1$.
b) $f(x) = 2x + 1$.
c) $f(x) = \lceil x / 5 \rceil$.
d) $f(x) = \lfloor (x^2 + 1) / 3 \rfloor$.

31. Soit $f(x) = \lfloor x^2 / 3 \rfloor$. Trouvez $f(S)$ si

a) $S = \{-2, -1, 0, 1, 2, 3\}$.
b) $S = \{0, 1, 2, 3, 4, 5\}$.
c) $S = \{1, 5, 7, 11\}$.
d) $S = \{2, 6, 10, 14\}$.

32. Soit $f(x) = 2x$ où le domaine est l'ensemble des nombres réels bers. Quel est

a) $f(\mathbf{Z})$?
b) $f(\mathbf{N})$?
c) $f(\mathbf{R})$?

33. Supposons que g est une fonction de A à B et f est un fonction de B à C.

a) Montrer que si f et g sont des fonctions biunivoque, alors $f \circ g$ est également un à un.

b) Montrer que si f et g sont sur des fonctions, alors $f \circ g$ est également sur.

∗ **34.** Si f et $f \circ g$ sont un à un, cela signifie-t-il que g est

Un par un? Justifiez votre réponse.

∗ **35.** Si f et $f \circ g$ sont sur, cela signifie-t-il que g est sur?

Justifiez votre réponse.

36. Trouvez $f \circ g$ et $g \circ f$, où $f(x) = x^2 + 1$ et $g(x) = x + 2$, sont des fonctions de **R** à **R**.

37. Trouvez $f + g$ et fg pour les fonctions f et g données dans Exercice 36.

38. Soit $f(x) = ax + b$ et $g(x) = cx + d$, où a, b, c, et d sont des constantes. Déterminer nécessaire et suffi-conditions appropriées sur les constantes a, b, c et d pour que $f \circ g = g \circ f$.

39. Montrer que la fonction $f(x) = ax + b$ de **R** à **R** est inversible, où a et b sont des constantes, avec $a = 0$, et trouver l'inverse de f.

40. Soit f une fonction de l'ensemble A à l'ensemble B. Soit S et T être sous - ensembles de A. Montre CA

a) $f(S \cup T) = f(S) \cup f(T)$.
b) $f(S \cap T) \subseteq f(S) \cap f(T)$.

41. a) Donnez un exemple pour montrer que l'inclusion dans la partie (b) dans l'exercice 40 peut être approprié.

b) Montrer que si f est un à un, l'inclusion dans la partie (b)

inverse de la fonction inversible f. Notez également que $f^{-1}(S)$, l'image inverse de l'ensemble S, a du sens pour toutes les fonctions f, pas seulement des fonctions inversibles.)

42. Soit f la fonction de **R** à **R** définie par $f(x) = x^2$. Trouver

a) $f^{-1}(\{1\})$.
b) $f^{-1}(\{x \mid 0 < x < 1\})$.
c) $f^{-1}(\{x \mid x > 4\})$.

43. Soit $g(x) = \lfloor x \rfloor$. Trouver

a) $g^{-1}(\{0\})$.
b) $g^{-1}(\{-1, 0, 1\})$.
c) $g^{-1}(\{x \mid 0 < x < 1\})$.

44. Soit f une fonction de A à B. Soit S et T *des* sous-ensembles de B. Montre CA

a) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$.
b) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

45. Soit f une fonction de A à B. Laissez S être un sous - ensemble de B. Montrer que $f^{-1}(S) = f^{-1}(S)$.

46. Montrer que $\lfloor x + \frac{1}{2} \rfloor$ est l'entier le plus proche du nombre x, sauf quand x est à mi-chemin entre deux entiers, quand il est le plus grand de ces deux nombres entiers.

47. Montrer que $\lceil x - \frac{1}{2} \rceil$ est l'entier le plus proche du nombre x, sauf quand x est à mi-chemin entre deux entiers, quand il est le plus petit de ces deux nombres entiers.

48. Montrer que si x est un nombre réel, alors $\lceil x \rceil - \lfloor x \rfloor = 1$ si x n'est pas un entier et $\lceil x \rceil - \lfloor x \rfloor = 0$ si x est un entier.

49. Montrer que si x est un nombre réel, alors $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.

50. Montrez que si x est un nombre réel et m est un entier, alors $\lceil x + m \rceil = \lceil x \rceil + m$.

51. Montrez que si x est un nombre réel et n est un entier, alors

a) $x < n$ si et seulement si $\lfloor x \rfloor < n$.
b) $n < x$ si et seulement si $n < \lceil x \rceil$.

52. Montrer que si x est un nombre réel et n est un entier, alors

a) $x \leq n$ si et seulement si $\lceil x \rceil \leq n$.
b) $n \leq x$ si et seulement si $n \leq \lfloor x \rfloor$.

53. Montrer que si n est un entier, alors $\lfloor n / 2 \rfloor = n / 2$ si n est pair et $(n - 1) / 2$ si n est impair.

54. Montrer que si x est un nombre réel, alors $\lfloor -x \rfloor = -\lceil x \rceil$ et $\lceil -x \rceil = -\lfloor x \rfloor$.

55. La fonction INT se trouve sur certaines calculatrices, où $\mathrm{INT}(x) = \lfloor x \rfloor$ lorsque x est un nombre réel non négatif et $\mathrm{INT}(x) = \lceil x \rceil$ lorsque x est un nombre réel négatif. Spectacle que cette fonction INT satisfait l'identité $\mathrm{INT}(-x) = -\mathrm{INT}(x)$.

56. Soit a et b des nombres réels avec $a < b$. Utilisez le sol et / ou des fonctions de plafond pour exprimer le nombre de dans l'exercice 40 est une égalité.

Soit f une fonction de l'ensemble A à l'ensemble B . Soit S un sous - ensemble de B . Nous définissons l' **image inverse** de S comme le sous-ensemble de A dont les éléments sont précisément toutes des pré-images de tous ments de S . On note l'image inverse de S par $f^{-1}(S)$, donc $f^{-1}(S) = \{ a \in A \mid f(a) \in S \}$. (*Attention:* la notation f^{-1} est utilisé de deux manières différentes. Ne confondez pas la notation ici avec la notation $f^{-1}(y)$ pour la valeur en y du

gers n qui satisfont l'inégalité $a \leq n \leq b$.

57. Soit a et b des nombres réels avec $a < b$. Utilisez le sol et / ou des fonctions de plafond pour exprimer le nombre de gers n qui satisfont l'inégalité $a < n < b$.

58. Combien d'octets sont nécessaires pour coder n bits de données où n est égal

a) 4? **b)** 10? **c)** 500? **d)** 3000?

59. Combien d'octets sont nécessaires pour coder n bits de données où n est égal

a) 7? **b)** 17? **c)** 1001? **d)** 28.800?

60. Combien de cellules ATM (décrites dans l'exemple 28) peuvent être transmis en 10 secondes sur une liaison fonctionnant au taux bas?

a) 128 kilobits par seconde (1 kilobit = 1000 bits)
b) 300 kilobits par seconde
c) 1 mégabit par seconde (1 mégabit = 1 000 000 bits)

61. Les données sont transmises sur un réseau Ethernet particulier en blocs de 1500 octets (blocs de 8 bits). Combien blocs sont nécessaires pour transmettre les quantités suivantes de des données sur ce réseau Ethernet? (Notez qu'un octet est un synonyme d'un octet, un kilo-octet est de 1000 octets et un mégaoctet est de 1000000 octets.)

a) 150 kilo-octets de données
b) 384 kilo-octets de données
c) 1,544 mégaoctets de données
d) 45,3 mégaoctets de données

62. Dessinez le graphique de la fonction $f(n) = 1 - n^2$ de **Z** à **Z** .

63. Tracer le graphique de la fonction $f(x) = \lfloor 2x \rfloor$ de **R** à **R** .

64. Tracez le graphique de la fonction $f(x) = \lfloor x/2 \rfloor$ à partir de **R** à **R** .

65. Tracez le graphique de la fonction $f(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor$ à partir de **R** à **R** .

66. Tracez le graphique de la fonction $f(x) = \lceil x \rceil + \lfloor x/2 \rfloor$ à partir de **R** à **R** .

67. Tracez des graphiques de chacune de ces fonctions.

a) $f(x) = \lfloor x + \frac{1}{2} \rfloor$ **b)** $f(x) = \lfloor 2x + 1 \rfloor$
c) $f(x) = \lceil x/3 \rceil$ **d)** $f(x) = \lceil 1/x \rceil$
e) $f(x) = \lceil x - 2 \rceil + \lfloor x + 2 \rfloor$
f) $f(x) = \lfloor 2x \rfloor \lceil x/2 \rceil$ **g)** $f(x) = \lceil \lfloor x - \frac{1}{2} \rfloor + \frac{1}{2} \rceil$

68. Tracez des graphiques de chacune de ces fonctions.

a) $f(x) = \lceil 3x - 2 \rceil$ **b)** $f(x) = \lceil 0.2x \rceil$
c) $f(x) = \lfloor -1/x \rfloor$ **d)** $f(x) = \lfloor x^2 \rfloor$
e) $f(x) = \lceil x/2 \rceil \lfloor x/2 \rfloor$ **f)** $f(x) = \lfloor x/2 \rfloor + \lceil x/2 \rceil$
g) $f(x) = \lfloor 2 \lceil x/2 \rceil + \frac{1}{2} \rfloor$

69. Trouvez la fonction inverse de $f(x) = x^3 + 1$.

70. Supposons que f soit une fonction inversible de Y à Z et g est une fonction inversible de X à Y . Spectacle que l'inverse de la composition $f \circ g$ est donné par $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

71. Soit S un sous - ensemble d'un ensemble universel U . La **caractéristique la fonction** f_S de S est la fonction de U vers l'ensemble $\{0, 1\}$ tel que $f_S(x) = 1$ si x appartient à S et $f_S(x) = 0$ si x ne fait pas partie S . Soit A et B *des* ensembles. Montrez cela pour tout $x \in U$,

a) $f_{A \cap B}(x) = f_A(x) \cdot f_B(x)$
b) $f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x)$
c) $f_{\overline{A}}(x) = 1 - f_A(x)$
d) $f_{A \oplus B}(x) = f_A(x) + f_B(x) - 2 f_A(x) f_B(x)$

72. Supposons que f soit une fonction de A à B , où A et B sont des ensembles finis avec $|A| = |B|$. Montrez que f est un à un si et seulement si c'est sur.

73. Prouvez ou réfutez chacune de ces déclarations sur la parole et fonctions de plafond.

a) $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ pour tous les nombres réels x .
b) $\lfloor 2x \rfloor = 2\lfloor x \rfloor$ chaque fois que x est un nombre réel.
c) $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil = 0$ ou 1 chaque fois que x et y sont nombres réels.
d) $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$ pour tous les nombres réels x et y .
e) $\left\lceil \frac{x}{2} \right\rceil = \left\lfloor \frac{x+1}{2} \right\rfloor$ pour tous les nombres réels x .

74. Prouvez ou réfutez chacune de ces déclarations sur la parole et fonctions de plafond.

a) $\lfloor \lceil x \rceil \rfloor = \lceil x \rceil$ pour tous les nombres réels x .
b) $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ pour tous les nombres réels x et y .
c) $\lceil \lceil x/2 \rceil / 2 \rceil = \lceil x/4 \rceil$ pour tous les nombres réels x .
d) $\lfloor \sqrt{\lceil x \rceil} \rfloor = \lfloor \sqrt{x} \rfloor$ pour tous les nombres réels positifs x .
e) $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$ pour tous réels les nombres x et y .

75. Montrer que si x est un nombre réel positif, alors

a) $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$.
b) $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$.

76. Soit x un nombre réel. Montrer que $\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{3} \rfloor + \lfloor x + \frac{2}{3} \rfloor$.

77. Pour chacune de ces fonctions partielles, déterminez son domaine, domaine de codage, domaine de définition et ensemble de valeurs pour dont il est indéfini. Déterminez également s'il s'agit d'un total une fonction.

a) $f : \mathbf{Z} \to \mathbf{R}$, $f(n) = 1/n$
b) $f : \mathbf{Z} \to \mathbf{Z}$, $f(n) = \lceil n/2 \rceil$
c) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Q}$, $f(m, n) = m/n$
d) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = mn$
e) $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $f(m, n) = m - n$ si $m > n$

78. a) Montrer qu'une fonction partielle de A à B peut être visualisée en fonction de f_* de A à $B \cup \{u\}$, où u n'est pas un élément de B et

$$f_*(a) = \begin{cases} f(a) & \text{si } a \text{ appartient au domaine de définition de } f \\ u & \text{si } f \text{ n'est pas défini en } a . \end{cases}$$

b) En utilisant la construction de (a), trouvez la fonction f_* correspondant à chaque fonction partielle de l'exercice 77.

79. a) Montrer que si un ensemble S a la cardinalité m , où m est un entier positif, il y a alors une correspondance biunivoque dence entre S et l'ensemble $\{1, 2, ..., m\}$.

b) Montrer que si S et T sont deux ensembles chacun avec m elements, où m est un entier positif, alors il y a un one-to-one correspondance entre S et T .

∗ **80.** Montrer qu'un ensemble S est infini si et seulement s'il y a un bon sous-ensemble A de S *de* telle sorte qu'il y ait une correspondance un à un dence entre A et S .

Séquences et sommations

introduction

Les séquences sont des listes d'éléments ordonnées, utilisées de nombreuses façons en mathématiques discrètes. Par exemple largement, ils peuvent être utilisés pour représenter des solutions à certains problèmes de comptage, comme nous le verrons dans Chapitre 8. Ils constituent également une structure de données importante en informatique. Nous aurons souvent besoin de travailler avec des sommes de termes de séquences dans notre étude des mathématiques discrètes. Cette section examine l'utilisation de la notation de sommation, les propriétés de base des sommations et les formules somme des termes de certains types particuliers de séquences.

Les termes d'une séquence peuvent être spécifiés en fournissant une formule pour chaque terme du séquence. Dans cette section, nous décrivons une autre façon de spécifier les termes d'une séquence en utilisant une relation de récurrence, qui exprime chaque terme comme une combinaison des termes précédents. nous présentera une méthode, appelée itération, pour trouver une formule fermée pour les termes d'un séquence spécifiée via une relation de récurrence. Identifier une séquence lors des premiers termes sont fournis est une compétence utile lors de la résolution de problèmes en mathématiques discrètes. Nous fournirons quelques conseils, y compris un outil utile sur le Web, pour ce faire.

Les séquences

Une séquence est une structure discrète utilisée pour représenter une liste ordonnée. Par exemple, 1, 2, 3, 5, 8 est une séquence de cinq termes et 1, 3, 9, 27, 81, ... , 3^n, ... est une séquence infinie.

DÉFINITION 1 Une *séquence* est une fonction d'un sous-ensemble de l'ensemble des entiers (généralement soit l'ensemble $\{0, 1, 2, \ldots\}$ ou l'ensemble $\{1, 2, 3, \ldots\}$) pour un ensemble S. Nous utilisons la notation a_n pour désigner l'image de l'entier n. Nous appelons a_n un *terme* de la séquence.

Nous utilisons la notation $\{a_n\}$ pour décrire la séquence. (Notez que *un* $_n$ représente un individu terme de la séquence $\{a_n\}$. Sachez que la notation $\{a_n\}$ d'une séquence est en conflit avec le notation pour un ensemble. Cependant, le contexte dans lequel nous utilisons cette notation indiquera toujours clairement quand nous avons affaire à des ensembles et quand nous avons affaire à des séquences. De plus, bien que nous avoir utilisé la lettre a dans la notation d'une séquence, d'autres lettres ou expressions peuvent être utilisées en fonction de la séquence considérée. Autrement dit, le choix de la lettre a est arbitraire.)

Nous décrivons les séquences en listant les termes de la séquence par ordre croissant d'indices.

EXEMPLE 1 Considérons la séquence $\{a_n\}$, où

$$a_n = \frac{1}{n}.$$

La liste des termes de cette séquence, commençant par *un* $_1$, à savoir,

$$a_1, a_2, a_3, a_4, \ldots,$$

commence avec

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots .$$

▲

DÉFINITION 2 Une *progression géométrique* est une séquence de la forme

$$a, ar, ar^2, ..., ar^n, ...$$

où le *terme initial a* et le *rapport commun r* sont des nombres réels.

Remarque: Une progression géométrique est un analogue discret de la fonction exponentielle $f(x) = ar^x$.

EXEMPLE 2 Les séquences $\{b_n\}$ avec $b_n = (-1)^n$, $\{c_n\}$ avec $c_n = 2 \cdot 5^n$ Et $\{d_n\}$ avec $d_n = 6 \cdot (1/\text{trois})^n$ sont progressions géométriques à terme initial et rapport commun égal à 1 et -1;2 et 5; et 6 et 1 / 3, respectivement, si on commence à $n = 0$. La liste des termes b_0, b_1, b_2, b_3, b_4, ... commence par

$$1, -1, 1, -1, 1, ...;$$

la liste des termes c_0, c_1, c_2, c_3, c_4, ... commence par

$$2, 10, 50, 250, 1250, ...;$$

et la liste des termes d_0, d_1, d_2, d_3, d_4, ... commence par

$$6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, ...$$ ▲

DÉFINITION 3 Une *progression arithmétique* est une séquence de la forme

$$a, a + d, a + 2d, ..., a + nd, ...$$

où le *terme initial a* et la *différence commune d* sont des nombres réels.

Remarque: Une progression arithmétique est un analogue discret de la fonction linéaire $f(x) = dx + a$.

EXEMPLE 3 Les séquences $\{s_n\}$ avec $s_n = -1 + 4n$ et $\{t_n\}$ avec $t_n = 7 - 3n$ sont toutes deux des progressions arithmétiques. avec des termes initiaux et des différences communes égales respectivement à -1 et 4, et 7 et -3, si on commence à $n = 0$. La liste des termes s_0, s_1, s_2, s_3, ... commence par

$$-1, 3, 7, 11, ...,$$

et la liste des termes t_0, t_1, t_2, t_3, ... commence par

$$7, 4, 1, -2, ...$$ ▲

Les séquences de la forme $a_1, a_2, ..., a_n$ sont souvent utilisées en informatique. Ces finis les séquences sont également appelées **chaînes** . Cette chaîne est également désignée par $a_1 a_2 ... a_n$. (Rappelez-vous ce bit chaînes, qui sont des séquences finies de bits, ont été introduites dans la section 1.1.) La **longueur** d'un chaîne est le nombre de termes de cette chaîne. La **chaîne vide** , notée λ , est la chaîne qui n'a pas de conditions. La chaîne vide a une longueur nulle.

EXEMPLE 4 La chaîne *abcd* est une chaîne de longueur quatre. ▲

Relations de récurrence

Dans les exemples 1 à 3, nous avons spécifié des séquences en fournissant des formules explicites pour leurs termes.Là existe de nombreuses autres façons de spécifier une séquence. Par exemple, une autre façon de spécifier une séquence est pour fournir un ou plusieurs termes initiaux ainsi qu'une règle pour déterminer les termes suivants ceux qui les précèdent.

DÉFINITION 4 Une *relation de récurrence* pour la séquence $\{a_n\}$ est une équation qui exprime un_n en termes de un ou plusieurs des termes précédents de la séquence, à savoir, un_0, un_1, ..., un_{n-1}, pour tous les entiers n avec $n \geq n_0$, où n_0 est un entier non négatif. Une séquence est appelée une *solution* d'une récurrence si ses termes satisfont la relation de récurrence. (Une relation de récurrence est dite *récursivement définir* une séquence. Nous expliquerons cette terminologie alternative au chapitre 5.)

EXEMPLE 5 Soit $\{a_n\}$ une séquence qui satisfait la relation de récurrence $a_n = a_{n-1} + 3$ pour $n = 1, 2, 3, ...,$ et supposons que $a_0 = 2$. Que sont un_1, un_2 et un_3 ?

Solution: Nous voyons d'après la relation de récurrence que $a_1 = a_0 + 3 = 2 + 3 = 5$. Il suit alors qui $a_2 = 3 + 5 = 8$ et $un_3 = 8 + 3 = 11$. ▲

EXEMPLE 6 Soit $\{a_n\}$ une séquence satisfaisant la relation de récurrence $a_n = a_{n-1} - a_{n-2}$ pour $n = 2, 3, 4, ...,$ et supposons que $un_0 = 3$ et $un_1 = 5$. Quels sont un_2 et un_3 ?

Solution: Nous voyons d'après la relation de récurrence que $a_2 = a_1 - a_0 = 5 - 3 = 2$ et $a_3 = a_2 - a_1 = 2 - 5 = -3$. On peut trouver un_4, un_5 et chaque terme successif de manière similaire. ▲

Les **conditions initiales** d'une séquence définie récursivement spécifient les termes qui précèdent le premier terme où la relation de récurrence prend effet. Par exemple, la condition initiale de l'exemple 5 est $un_0 = 2$, et les conditions initiales de l'exemple 6 sont $un_0 = 3$ et $un_1 = 5$. Utilisation de mathématiques l'induction, une technique de preuve présentée au chapitre 5, on peut montrer qu'une relation de récurrence avec ses conditions initiales détermine une solution unique.

Sautez jusqu'au chapitre 8 apprendre à trouver un formule pour le Fibonacci Nombres.

Ensuite, nous définissons une séquence particulièrement utile définie par une relation de récurrence, connue sous le nom la **séquence de Fibonacci**, d'après le mathématicien italien Fibonacci né le 12 siècle (voir le chapitre 5 pour sa biographie). Nous étudierons cette séquence en profondeur dans les chapitres 5 et 8, où nous verrons pourquoi il est important pour de nombreuses applications, y compris la modélisation de la croissance démographique des lapins.

DÉFINITION 5 La *séquence de Fibonacci*, $f_0, f_1, f_2, ...,$ est définie par les conditions initiales $f_0 = 0$, $f_1 = 1$, et la relation de récurrence

$$f_n = f_{n-1} + f_{n-2}$$

pour $n = 2, 3, 4, ...$

EXEMPLE 7 Trouver les nombres de Fibonacci f_2, f_3, f_4, f_5 et f_6.

Solution: La relation de récurrence pour la séquence de Fibonacci nous dit que nous trouvons successives termes en ajoutant les deux termes précédents. Parce que les conditions initiales nous disent que $f_0 = 0$ et $f_1 = 1$, en utilisant la relation de récurrence dans la définition, nous constatons que

$$f_2 = f_1 + f_0 = 1 + 0 = 1,$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2,$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3,$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5,$$
$$f_6 = f_5 + f_4 = 5 + 3 = 8.$$

▲

EXEMPLE 8 Supposons que $\{a_n\}$ est la séquence d'entiers définie par $a_n = n!$, La valeur de la factorielle fonction à l'entier n, où $n = 1, 2, 3, ...$. Parce que $n! = n((n-1)(n-2) \ldots 2 \cdot 1) =$

$n(n-1)! = na_{n-1}$, on voit que la séquence des factorielles satisfait la relation de récurrence $a_n = na_{n-1}$, avec la condition initiale $a_1 = 1$. ▲

Nous disons que nous avons résolu la relation de récurrence avec les conditions initiales lorsque nous trouvons une formule explicite, appelée **formule fermée** , pour les termes de la séquence.

EXEMPLE 9 Déterminer si la séquence $\{a_n\}$, où $a_n = 3n$ pour chaque entier non négatif n, est un solution de la relation de récurrence $a_n = 2a_{n-1} - un_{n-2}$ pour $n = 2, 3, 4, \ldots$. Répondez pareil question où $a_n = 2^n$ et où $a_n = 5$.

Solution: Supposons que $a_n = 3n$ pour chaque entier non négatif n. Ensuite, pour $n \geq 2$, on voit que $2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3n = a_n$. Par conséquent, $\{a_n\}$, où $a_n = 3n$, est un solution de la relation de récurrence.

Supposons que $a_n = 2^n$ pour chaque entier non négatif n. Notez que $un_0 = 1$, $a_1 = 2$, et $une_2 = 4$. Parce que $2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$, nous voyons que $\{a_n\}$, où $a_n = 2^n$, n'est pas une solution de la relation de récurrence.

Supposons que $a_n = 5$ pour chaque entier non négatif n. Alors pour $n \geq 2$, on voit que $a_n = 2a_{n-1} - a_{n-2} = 2{,}5 \cdot 5 = 5 = a_n$. Par conséquent, $\{a_n\}$, où $a_n = 5$, est une solution de la récurrence relation de référence. ▲

De nombreuses méthodes ont été développées pour résoudre les relations de récurrence.Ici, nous allons présenter une méthode simple appelée itération via plusieurs exemples. Dans le chapitre 8, nous étudierons relations de récurrence en profondeur. Dans ce chapitre, nous montrerons comment les relations de récurrence peuvent être utilisées pour résoudre les problèmes de comptage et nous présenterons plusieurs méthodes puissantes qui peuvent être utilisées pour résoudre de nombreuses relations de récurrence différentes.

EXEMPLE 10 Résoudre la relation de récurrence et la condition initiale dans l'exemple 5.

Solution: on peut appliquer successivement la relation de récurrence dans l'exemple 5, en commençant par le condition initiale $a_1 = 2$, et travaillant vers le haut jusqu'à ce que nous atteignions un_n pour déduire une formule fermée pour la séquence. On voit ça

$$
\begin{aligned}
a_2 &= 2 + 3 \\
a_3 &= (2 + 3) + 3 = 2 + 3 \cdot 2 \\
a_4 &= (2 + 2 \cdot 3) + 3 = 2 + 3 \cdot 3 \\
&\ \ \vdots \\
a_n &= a_{n-1} + 3 = (2 + 3 \cdot (n-2)) + 3 = 2 + 3(n-1).
\end{aligned}
$$

On peut également appliquer successivement la relation de récurrence dans l'exemple 5, en commençant par le terme a_n et travaillant vers le bas jusqu'à ce que nous atteignions la condition initiale $a_1 = 2$ pour déduire ce même formule. Les étapes sont

$$
\begin{aligned}
a_n &= a_{n-1} + 3 \\
&= (a_{n-2} + 3) + 3 = a_{n-2} + 3 \cdot 2 \\
&= (a_{n-3} + 3) + 3 \cdot 2 = a_{n-3} + 3 \cdot 3 \\
&\ \ \vdots \\
&= a_2 + 3(n-2) = (a_1 + 3) + 3(n-2) = 2 + 3(n-1).
\end{aligned}
$$

À chaque itération de la relation de récurrence, nous obtenons le terme suivant dans la séquence par ajouter 3 au terme précédent. On obtient le n ème terme après $n - 1$ itérations de la récurrence relation. Par conséquent, nous avons ajouté $3(n-1)$ au terme initial $a_0 = 2$ pour obtenir un_n. Cela nous donne la formule fermée $a_n = 2 + 3(n-1)$. Notez que cette séquence est une progression arithmétique. ▲

La technique utilisée dans l'exemple 10 est appelée **itération** . Nous avons répété, ou utilisé à plusieurs reprises, la relation de récurrence. La première approche est appelée **substitution directe** - nous avons trouvé successives termes commençant par la condition initiale et se terminant par un_n. La deuxième approche est appelée **substitution en arrière** , parce que nous avons commencé par un_n et itéré pour l'exprimer en termes de chute termes de la séquence jusqu'à ce que nous l' avons trouvé en termes d' un_1. Notez que lorsque nous utilisons l'itération, nous devinez une formule pour les termes de la séquence.Pour prouver que notre supposition est correcte, nous besoin d'utiliser l'induction mathématique, une technique dont nous discutons au chapitre 5.

Au chapitre 8, nous montrerons que les relations de récurrence peuvent être utilisées pour modéliser une grande problèmes. Nous fournissons ici un exemple, montrant comment utiliser une relation de récurrence pour trouver intérêts composés.

EXEMPLE 11 **Intérêt composé** Supposons qu'une personne dépose 10 000 $ dans un compte d'épargne dans une banque rendement de 11% par an avec intérêts composés annuellement.Combien sera dans le compte après 30 ans?

Solution: Pour résoudre ce problème, considérons P_n le montant du compte après n années. Car le montant dans le compte après n ans est égal au montant dans le compte après $n - 1$ ans plus intérêt pour la n ème année, on voit que la séquence $\{P_n\}$ satisfait la relation de récurrence

$$P_n = P_{n-1} + 0.11 P_{n-1} = (1.11) P_{n-1}.$$

L'état initial est $P_0 = 10,000$.

Nous pouvons utiliser une approche itérative pour trouver une formule pour P_n. Notez que

$$P_1 = (1.11) P_0$$
$$P_2 = (1.11) P_1 = (1.11)^2 P_0$$
$$P_3 = (1.11) P_2 = (1.11)^3 P_0$$
$$\ldots$$
$$P_n = (1.11) P_{n-1} = (1.11)^n P_0.$$

Quand on insère la condition initiale $P_0 = 10,000$, la formule $P_n = (1.11)^n 10,000$ est obtenue.

Insertion $n = 30$ dans la formule $P_n = (1.11)^n 10,000$ montre qu'après 30 ans , le compte contient

$$P_{30} = (1.11)^{30} 10,000 = 228 \$, 922.97.$$

▲

Séquences entières spéciales

Un problème courant en mathématiques discrètes est de trouver une formule fermée, une relation de récurrence, ou un autre type de règle générale pour construire les termes d'une séquence.Parfois seulement peu de termes d'une séquence résolvant un problème sont connus; le but est d'identifier la séquence.Même bien que les termes initiaux d'une séquence ne déterminent pas la séquence entière (après tout, il y a infiniment de séquences différentes qui commencent par un ensemble fini de termes initiaux), connaissant les premiers termes peuvent vous aider à faire une conjecture éclairée sur l'identité de votre séquence. Une fois que vous avez fait cette conjecture, vous pouvez essayer de vérifier que vous avez la bonne séquence.

Lorsque vous essayez de déduire une formule possible, une relation de récurrence ou un autre type de règle pour les termes d'une séquence lorsque les termes initiaux sont donnés, essayez de trouver un modèle dans ces termes.Vous pourrait également voir si vous pouvez déterminer comment un terme a pu être produit à partir de ceux le précédant. Il y a beaucoup de questions que vous pourriez poser, mais certaines des plus utiles sont:

- Y a-t-il des séries de la même valeur?Autrement dit, la même valeur se produit-elle plusieurs fois dans un rangée?
- Les conditions sont-elles obtenues à partir des conditions précédentes en ajoutant le même montant ou un montant qui dépend de la position dans la séquence?
- Les termes sont-ils obtenus à partir des termes précédents en multipliant par un montant particulier?
- Les termes sont-ils obtenus en combinant les termes précédents d'une certaine manière?
- Y a-t-il des cycles parmi les termes?

EXEMPLE 12 formules de trouver pour les séquences de ce qui suit première cinq conditions: (a) 1, 1 / 2, 1 / 4, 1 / 8, 1 / 16 (b) 1, 3, 5, 7, 9 (c) 1, -1, 1, -1, 1.

Solution: (a) Nous reconnaissons que les dénominateurs sont des puissances de 2. La séquence avec $un_n = 1 / 2^n$, $n = 0, 1, 2, \ldots$ est une correspondance possible. Cette séquence proposée est une progression géométrique avec $un = 1$ et $r = 1 / 2$.

(b) Nous notons que chaque terme est obtenu en ajoutant 2 au terme précédent.La séquence avec $un_n = 2n + 1$, $n = 0, 1, 2, \ldots$ est une correspondance possible. Cette séquence proposée est une arithmétique progression avec $a = 1$ et $d = 2$.

(c) Les termes alternent entre 1 et -1.La séquence avec $une_n = (-1)^n$, $n = 0, 1, 2 \ldots$ est une correspondance possible. Cette séquence proposée est une progression géométrique avec $a = 1$ et $r = -1$.

▲

Les exemples 13 à 15 illustrent comment analyser des séquences pour trouver comment les termes sont structuré.

EXEMPLE 13 Comment produire les termes d'une séquence si les 10 premiers termes sont 1, 2, 2, 3, 3, 3, 4, 4, 4, 4?

Solution: dans cette séquence, l'entier 1 apparaît une fois, l'entier 2 apparaît deux fois, l'entier 3 apparaît trois fois et l'entier 4 apparaît quatre fois. Une règle raisonnable pour générer ce la séquence est que l'entier n apparaît exactement n fois, donc les cinq prochains termes de la séquence serait tous 5, les six termes suivants seraient tous 6, et ainsi de suite. La séquence a généré ce est une correspondance possible. ▲

EXEMPLE 14 Comment produire les termes d'une séquence si les 10 premiers termes sont 5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

Solution: Notez que chacun des 10 premiers termes de cette séquence après le premier est obtenu en ajoutant 6 au terme précédent. (Nous avons pu le constater en remarquant que la différence entre des termes est 6.) Par conséquent, le n ème terme pourrait être produit en commençant par 5 et en ajoutant 6 a total de n - 1 fois; c'est-à-dire, une supposition raisonnable est que le n ème terme est $5 + 6(n - 1) = 6n - 1$. (Il s'agit d'une progression arithmétique avec $a = 5$ et $d = 6$.) ▲

EXEMPLE 15 Comment produire les termes d'une séquence si les 10 premiers termes sont 1, 3, 4, 7, 11, 18, 29, 47, 76, 123?

Solution: observez que chaque terme successif de cette séquence, en commençant par le troisième terme, est la somme des deux termes précédents. Autrement dit, 4 = 3 + 1, 7 = 4 + 3, 11 = 7 + 4, et ainsi de suite. Par conséquent, si L_n est le n ème terme de cette séquence, on suppose que la séquence est déterminée par la relation de récurrence $L_n = L_{n-1} + L_{n-2}$ avec les conditions initiales $L_1 = 1$ et $L_2 = 3$ (le

TABLEAU 1 **Quelques séquences utiles.**

nième terme	*10 premiers termes*
n^2	1 , 4 , 9 , 16 , 25 , 36 , 49 , 64 , 81 , 100 , ...
n^3	1 , 8 , 27 , 64 , 125 , 216 , 343 , 512 , 729 , 1000 , ...
n^4	1 , 16 , 81 , 256 , 625 , 1296 , 2401 , 4096 , 6561 , 10000 , ...
2^n	2 , 4 , 8 , 16 , 32 , 64 , 128 , 256 , 512 , 1024 , ...
3^n	3 , 9 , 27 , 81 , 243 , 729 , 2187 , 6561 , 19683 , 59049 , ...
$n!$	1 , 2 , 6 , 24 , 120 , 720 , 5040 , 40320 , 362880 , 3628800 , ...
f_n	1 , 1 , 2 , 3 , 5 , 8 , 13 , 21 , 34 , 55 , 89 , ...

même relation de récurrence que la séquence de Fibonacci, mais avec des conditions initiales différentes). Cette séquence est connue comme la **séquence de Lucas** , après le mathématicien français François Édouard Lucas. Lucas a étudié cette séquence et la séquence de Fibonacci au XIXe siècle. ▲

Une autre technique utile pour trouver une règle pour générer les termes d'une séquence consiste à comparer les termes d'une séquence d'intérêt avec les termes d'une séquence entière bien connue, comme les termes d'une progression arithmétique, les termes d'une progression géométrique, les carrés parfaits, cubes parfaits, etc. Les 10 premiers termes de certaines séquences que vous voudrez peut-être garder à l'esprit sont affichés dans le tableau 1.

EXEMPLE 16 Conjecture d'une formule simple pour un a_n si les 10 premiers termes de la séquence $\{a_n\}$ sont 1, 7, 25, 79, 241, 727, 2185, 6559, 19681, 59047.

Solution: Pour attaquer ce problème, nous commençons par regarder la différence de termes consécutifs, mais nous ne voyons pas de modèle. Lorsque nous formons le rapport des termes consécutifs pour voir si chacun terme est un multiple du terme précédent, nous constatons que ce rapport, bien que non constant, est proche à 3. Il est donc raisonnable de soupçonner que les termes de cette séquence sont générés par une formule impliquant 3^n. Comparaison de ces termes avec les termes correspondants de la séquence $\{3^n\}$, nous notons que le n ème terme est 2 de moins que la puissance correspondante de 3. On voit que $a_n = 3^n - 2$ pour $1 \leq n \leq 10$ et conjecture que cette formule est valable pour tout n . ▲

Nous verrons tout au long de ce texte que des séquences entières apparaissent dans un large éventail de contextes Mathématiques discrètes. Les séquences que nous avons rencontrées ou rencontrerons incluent la séquence nombre de nombres premiers (chapitre 4), le nombre de façons d'ordonner n objets discrets (chapitre 6), nombre de mouvements nécessaires pour résoudre le célèbre puzzle de la Tour de Hanoi avec n disques (Chapitre 8), et le nombre de lapins sur une île après n mois (chapitre 8).

Découvrez les puzzles sur le site OEIS.

Les séquences entières apparaissent dans un éventail incroyablement large de sujets en plus de discrètes mathématiques, y compris la biologie, l'ingénierie, la chimie et la physique, ainsi que dans les puzzles. Un une base de données étonnante de plus de 200 000 séquences entières différentes peut être trouvée dans le *On-Line Encyclopédie des séquences entières (OEIS)* . Cette base de données a été créée par Neil Sloane dans le Années 60. La dernière version imprimée de cette base de données a été publiée en 1995 ([SIPI95]); le courant l'encyclopédie occuperait plus de 750 volumes de la taille du livre de 1995 avec plus de 10 000 nouvelles soumissions par an. Il existe également un programme accessible via le Web que vous pouvez utiliser pour trouver des séquences de l'encyclopédie qui correspondent aux termes initiaux que vous fournissez.

Sommations

Ensuite, nous considérons l'ajout des termes d'une séquence. Pour cela, nous introduisons la **sommation notation** . Nous commençons par décrire la notation utilisée pour exprimer la somme des termes

$$a_m, a_{m+1}, \ldots, a_n$$

à partir de la séquence $\{a_n\}$. Nous utilisons la notation

$$\sum_{j=m}^{n} a_j, \qquad \sum\nolimits_{j=m}^{n} a_j, \qquad \text{ou} \qquad \sum_{m \le j \le n} a_j$$

(lu comme la somme de $j = m$ à $j = n$ d' a_j) pour représenter

$$a_m + a_{m+1} + \cdots + a_n .$$

Ici, la variable j est appelée l' **indice de sommation** , et le choix de la lettre j comme la variable est arbitraire; c'est-à-dire que nous aurions pu utiliser n'importe quelle autre lettre, comme i ou k . Ou, en notation,

$$\sum_{j=m}^{n} a_j = \sum_{i=m}^{n} a_i = \sum_{k=m}^{n} a_k .$$

Ici, l'index de sommation parcourt tous les entiers commençant par sa **limite inférieure** m et se terminant avec sa **limite supérieure** n . Une grande lettre grecque majuscule sigma, $\sum$, est utilisé pour désigner la sommation.

Les lois habituelles pour l'arithmétique s'appliquent aux sommations. Par exemple, lorsque a et b sont réels chiffres, nous avons $\sum_{j=1}^{n} (ax_j + \text{par}_j) = a \sum_{y=1}^{n} x_j + b \sum_{j=1}^{n} y_j$, où $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_n$ sont des nombres réels. (Nous ne présentons pas ici de preuve formelle de cette identité. Une telle La preuve peut être construite par induction mathématique, une méthode de preuve que nous introduisons ter 5. La preuve utilise également les lois commutatives et associatives pour l'addition et la distribution loi de multiplication sur l'addition.)

Nous donnons quelques exemples de notation de sommation.

EXEMPLE 17 Utiliser la notation de sommation pour exprimer la somme des 100 premiers termes de la séquence $\{a_j\}$, où $a_j = 1/j$ pour $j = 1, 2, 3, \ldots$.

Solution: la limite inférieure de l'index de sommation est 1 et la limite supérieure est 100. Nous écrivons cette somme

$$\sum_{j=1}^{100} \frac{1}{j} .$$

▲

NEIL SLOANE (NÉ EN 1939) Neil Sloane a étudié les mathématiques et le génie électrique à l'Université de Melbourne grâce à une bourse de la compagnie de téléphone publique australienne. Il a maîtrisé beaucoup emplois liés au téléphone, tels que la construction de poteaux téléphoniques, dans son travail d'été. Après avoir obtenu son diplôme, il a conçu réseaux téléphoniques à moindre coût en Australie. En 1962, il est venu aux États-Unis et a étudié l'électri-génie civil à l'Université Cornell. Son doctorat. thèse portait sur ce que l'on appelle aujourd'hui les réseaux de neurones. Il a pris un emploi aux Bell Labs en 1969, travaillant dans de nombreux domaines, y compris la conception de réseaux, la théorie du codage et emballage de sphère. Il travaille maintenant pour AT&T Labs, y déménageant de Bell Labs lorsque AT&T s'est séparé en 1996. L'un de ses problèmes préférés est le **problème des baisers** (un nom qu'il a inventé), qui demande combien les sphères peuvent être disposées en n dimensions afin qu'elles touchent toutes une sphère centrale de même taille. (En deux dimensions, la réponse est 6, car 6 pièces peuvent être placées de manière à toucher un sou central. En trois dimensions, 12 billard les boules peuvent être placées de manière à ce qu'elles touchent une boule centrale de billard. On dit que deux boules de billard qui viennent de toucher «s'embrassent», terminologie «problème de baisers» et «nombre de baisers».) Sloane, avec Andrew Odlyzko, a montré qu'en 8 et 24 dimensions, les nombres optimaux de baisers sont respectivement 240 et 196 560. Le nombre de baisers est connu dans les dimensions 1, 2, 3, 4, 8 et 24, mais pas dans d'autres dimensions. Les livres de Sloane incluent *Sphere Packings, Lattices and Groups,* 3d ed., Avec John Conway; *La théorie des codes de correction d'erreurs* avec Jessie MacWilliams; *L'Encyclopédie des séquences entières* avec Simon Plouffe (qui a grandi dans le célèbre site Web OEIS); et *The Rock-Climbing Guide to New Jersey Crags* avec Paul Nick. Le dernier livre montre son intérêt pour l'escalade; il comprend plus de 50 sites d'escalade dans le New Jersey.

EXEMPLE 18 Quelle est la valeur de $\sum_{j=1}^{5} j^2$?

Solution: nous avons

$$\sum_{j=1}^{5} j^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$
$$= 1 + 4 + 9 + 16 + 25$$
$$= 55.$$

▲

EXEMPLE 19 Quelle est la valeur de $\sum_{k=4}^{8} (-1)^k$?

Solution: nous avons

$$\sum_{k=4}^{8} (-1)^k = (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8$$
$$= 1 + (-1) + 1 + (-1) + 1$$
$$= 1.$$

▲

Parfois, il est utile de déplacer l'indice de sommation dans une somme.Cela se fait souvent lorsque deux sommes doivent être ajoutées mais leurs indices de sommation ne correspondent pas. Lors du déplacement d'un index de sommation, il est important de faire les changements appropriés dans la sommation correspondante. Ceci est illustré par l'exemple 20.

EXEMPLE 20 Supposons que nous ayons la somme

$$\sum_{j=1}^{5} j^2$$

mais souhaitez que l'index de sommation s'exécute entre 0 et 4 plutôt que de 1 à 5. Pour ce faire, nous laissons $k = j - 1$. Ensuite, le nouvel indice de sommation va de 0 (car $k = 1 - 0 = 0$ lorsque $j = 1$) à 4 (car $k = 5 - 1 = 4$ lorsque $j = 5$), et le terme j^2 devient $(k + 1)^2$. Par conséquent,

$$\sum_{j=1}^{5} j^2 = \sum_{k=0}^{4} (k + 1)^2.$$

Il est facile de vérifier que les deux sommes sont 1 + 4 + 9 + 16 + 25 = 55. ▲

Des sommes de termes de progressions géométriques apparaissent généralement (ces sommes sont appelées **géométriques série**). Le théorème 1 nous donne une formule pour la somme des termes d'une progression géométrique.

THÉORÈME 1 Si a et r sont des nombres réels et $r = 0$, alors

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1} - a}{r - 1} & \text{si } r = 1 \\ (n + 1)a & \text{si } r = 1. \end{cases}$$

Preuve: Soit

$$S_n = \sum_{j=0}^{n} ar^j.$$

Pour calculer S , multipliez d'abord les deux côtés de l'égalité par r , puis manipulez le résultat additionner comme suit:

$$\begin{aligned}
rS_n &= r\sum_{j=0}^{n} ar^j && \text{substitution de la formule de sommation à } S\\
&= \sum_{j=0}^{n} ar^{j+1} && \text{par la propriété distributive}\\
&= \sum_{k=1}^{n+1} ar^k && \text{décalage de l'indice de sommation, avec } k = j + 1\\
&= \left(\sum_{k=0}^{n} ar^k\right) + (ar^{n+1} - a) && \text{supprimer } k = n + 1 \text{ terme et ajouter } k = 0 \text{ terme}\\
&= S_n + (ar^{n+1} - a) && \text{substitution de } S \text{ à la formule de sommation}
\end{aligned}$$

De ces égalités, nous voyons que

$$rS_n = S_n + (ar^{n+1} - a).$$

La résolution de S_n montre que si r = 1, alors

$$S_n = \frac{ar^{n+1} - a}{r - 1}.$$

Si $r = 1$, alors $S_n = \sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} a = (n + 1)a$.

EXEMPLE 21 Des doubles sommations se produisent dans de nombreux contextes (comme dans l'analyse des boucles imbriquées dans l'ordinateur programmes). Un exemple de double sommation est

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij.$$

Pour évaluer la double somme, développez d'abord la somme intérieure, puis continuez en calculant la sommation extérieure:

$$\begin{aligned}
\sum_{i=1}^{4}\sum_{j=1}^{3} ij &= \sum_{i=1}^{4} (i + 2i + 3i)\\
&= \sum_{i=1}^{4} 6i\\
&= 6 + 12 + 18 + 24 = 60.
\end{aligned}$$

▲

Nous pouvons également utiliser la notation de sommation pour ajouter toutes les valeurs d'une fonction ou les termes d'un index set, où l'index de sommation s'exécute sur toutes les valeurs d'un ensemble. Autrement dit, nous écrivons

$$\sum_{s \in S} f(s)$$

pour représenter la somme des valeurs $f(s)$, pour tous les membres s de S .

TABLEAU 2 **Quelques formules de sommation utiles.**

Somme	***Formulaire fermé***
$\sum_{k=0}^{n} ar^k \ (r = 0)$	$\frac{ar^{n+1} - a}{r - 1}, \ r = 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \ \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \ \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

EXEMPLE 22 Quelle est la valeur de $\sum_{s \in \{0, 2, 4\}} s$?

Solution: Parce que $\sum_{s \in \{0, 2, 4\}} s$ représente la somme des valeurs de s pour tous les membres du set $\{0, 2, 4\}$, il s'ensuit que

$$\sum_{s \in \{0, 2, 4\}} s = 0 + 2 + 4 = 6.$$

▲

Certaines sommes surviennent à plusieurs reprises au cours de mathématiques discrètes. Avoir une collection de des formules pour de telles sommes peuvent être utiles;Le tableau 2 présente un petit tableau de formules pour les sommes survenues.

Nous avons dérivé la première formule de ce tableau dans le théorème 1. Les trois formules suivantes nous donnent la somme des n premiers entiers positifs, la somme de leurs carrés et la somme de leurs cubes.Celles-ci trois formules peuvent être dérivées de différentes manières (par exemple, voir les exercices 37 et 38). Notez également que chacune de ces formules, une fois connue, peut facilement être prouvée en utilisant l'induction, objet de la section 5.1. Les deux dernières formules du tableau impliquent des séries infinies et sera discuté sous peu.

L'exemple 23 illustre l'utilité des formules du tableau 2.

EXEMPLE 23 Rechercher $\sum_{k=50}^{100} k^2$.

Solution: notez tout d'abord que $\sum_{k=1}^{100} k^2 = \sum_{k=1}^{49} k^2 + \sum_{k=50}^{100} k^2$, nous avons

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2.$$

Utilisation de la formule $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$ du tableau 2 (et prouvé dans l'exercice 38), on voit ça

$$\sum_{k=50}^{100} k^2 = \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6} = 338,350 - 40,425 = 297,925.$$

▲

QUELQUES SÉRIES INFINIES Bien que la plupart des sommations de ce livre soient des sommes finies, les séries infinies sont importantes dans certaines parties des mathématiques discrètes. Les séries infinies sont généralement étudié dans un cours de calcul et même la définition de ces séries nécessite l'utilisation du calcul, mais parfois ils surviennent en mathématiques discrètes, parce que les mathématiques discrètes traitent collections nies d'éléments discrets. En particulier, dans nos futures études en mathématiques discrètes, nous trouverons les formes fermées pour la série infinie dans les exemples 24 et 25 très utiles.

EXEMPLE 24 (*nécessite un calcul*) Soit x un nombre réel avec $|x| < 1$. Trouver $\sum_{n=0}^{\infty} x^n$.

Solution: Par le théorème 1 avec $a = 1$ et $r = x$, nous voyons que $\sum_{n=0}^{k} x^n = \frac{x^{k+1} - 1}{x - 1}$. Car $|x| < 1$, x^{k+1} s'approche de 0 lorsque k approche de l'infini Il s'ensuit que

$$\sum_{n=0}^{\infty} x^n = \lim_{k\to\infty} \frac{x^{k+1} - 1}{x - 1} = \frac{0 - 1}{x - 1} = \frac{1}{1 - x}.$$

▲

Nous pouvons produire de nouvelles formules de sommation en différenciant ou en intégrant des formules existantes.

EXEMPLE 25 (*nécessite un calcul*) Différenciation des deux côtés de l'équation

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1 - x},$$

à partir de l'exemple 24, nous constatons que

$$\sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1 - x)^2}.$$

(Cette différenciation est valable pour $|x| < 1$ par un théorème sur les séries infinies.) ▲

Des exercices

1. Trouvez ces termes de la séquence $\{a_n\}$, où $a_n = 2 \cdot (-3)^n + 5^n$.
a) un_0 **b)** un_1 **c)** un_4 **d)** un_5

2. Quel est le terme a_8 de la séquence $\{a_n\}$ si a_n est égal à
a) 2^{n-1} ? **b)** 7? **c)** $1 + (-1)^n$? **d)** $-(-2)^n$?

3. Quels sont les termes a_0, a_1, a_2 et a_3 de la séquence $\{a_n\}$, où a_n est égal
a) $2^n + 1$? **b)** $(n + 1)^{n+1}$? **c)** $\lfloor n/2 \rfloor$? **d)** $\lfloor n/2 \rfloor + \lceil n/2 \rceil$?

4. Quels sont les termes a_0, a_1, a_2 et a_3 de la séquence $\{a_n\}$, où a_n est égal
a) $(-2)^n$? **b)** 3? **c)** $7 + 4^n$? **d)** $2^n + (-2)^n$?

5. Énumérez les 10 premiers termes de chacune de ces séquences.
a) la séquence qui commence par 2 et dans laquelle chaque terme successif est 3 de plus que le terme précédent
b) la séquence qui répertorie chaque entier positif trois fois, dans l'ordre croissant
c) la séquence qui répertorie les entiers positifs impairs dans ordre de rainage, répertoriant chaque entier impair deux fois
d) la séquence dont le n ème terme est $n! - 2^n$
e) la séquence qui commence par 3, où chaque successeur terme est le double du terme précédent
f) la séquence dont le premier terme est 2, le deuxième terme est 4, et chaque terme suivant est la somme des deux pré- conditions de cession
g) la séquence dont le n ème terme est le nombre de bits dans l'expansion binaire du nombre n (défini dans Section 4.2)
h) la séquence où le n ème terme est le nombre de lettres ters dans le mot anglais pour l'index n

6. Énumérez les 10 premiers termes de chacune de ces séquences.
a) la séquence obtenue en commençant par 10 et en obtenant- chaque terme en soustrayant 3 du terme précédent
b) la séquence dont le n ème terme est la somme des n premiers entiers positifs
c) la séquence dont le n ème terme est $3^n - 2^n$
d) la séquence dont le n ème terme est $\lfloor \sqrt{n} \rfloor$
e) la séquence dont les deux premiers termes sont 1 et 5 et chaque terme suivant est la somme des deux précédents termes

f) la séquence dont le n ème terme est le plus grand entier dont l'expansion binaire (définie dans la section 4.2) a n bits (Écrivez votre réponse en notation décimale.)
g) la séquence dont les termes sont construits séquentiellement comme suit: commencez par 1, puis ajoutez 1, puis multipliez par 1, puis ajoutez 2, puis multipliez par 2, etc.
h) la séquence dont le n ème terme est le plus grand entier k tel que $k! \leq n$

7. Recherchez au moins trois séquences différentes commençant par termes 1, 2, 4 dont les termes sont générés par un simple mula ou règle.

8. Recherchez au moins trois séquences différentes commençant par termes 3, 5, 7 dont les termes sont générés par une simple mula ou règle.

9. Trouvez les cinq premiers termes de la séquence définie par chacun

c) $a_n = 3(-1)^n + 2^n - n + 2$.
d) $a_n = 7{,}2^n - n + 2$.

16. Trouver la solution à chacune de ces relations de récurrence avec les conditions initiales données. Utiliser une approche itérative telle que comme celle utilisée dans l'exemple 10.
a) $a_n = -a_{n-1}$, $a_0 = 5$
b) $a_n = a_{n-1} + 3$, $a_0 = 1$
c) $a_n = a_{n-1} - n$, $a_0 = 4$
d) $a_n = 2a_{n-1} - 3$, $a_0 = -1$
e) $a_n = (n + 1)a_{n-1}$, $a_0 = 2$
f) $a_n = 2na_{n-1}$, $a_0 = 3$
g) $a_n = -a_{n-1} + n - 1$, $a_0 = 7$

17. Trouver la solution à chacune de ces relations de récurrence et conditions initiales. Utilisez une approche itérative telle que celle utilisé dans l'exemple 10.

de ces relations de récurrence et conditions initiales.

a) $a_n = 6a_{n-1}$, $a_0 = 2$

b) $a_n = a^2_{n-1}$, $A_1 = 2$

c) $a_n = a_{n-1} + 3a_{n-2}$, $a_0 = 1$, $a_1 = 2$

d) $a_n = na_{n-1} + n^2 a_{n-2}$, $a_0 = 1$, $a_1 = 1$

e) $a_n = a_{n-1} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 0$

10. Trouvez les six premiers termes de la séquence définie par chacun de ces relations de récurrence et conditions initiales.

a) $a_n = -2a_{n-1}$, $a_0 = -1$

b) $a_n = a_{n-1} - a_{n-2}$, $a_0 = 2$, $a_1 = -1$

c) $a_n = 3a^2_{n-1}$, $a_0 = 1$

d) $a_n = na_{n-1} + a^2_{n-2}$, $a_0 = -1$, $a_1 = 0$

e) $a_n = a_{n-1} - a_{n-2} + a_{n-3}$, $a_0 = 1$, $a_1 = 1$, $a_2 = 2$

11. Soit $a_n = 2^n + 5 \cdot 3^n$ pour $n = 0, 1, 2, \ldots$.

a) Trouver un_0, un_1, un_2, un_3, et un_4.

b) Montrer que $a_2 = 5a_1 - 6a_0$, $a_3 = 5a_2 - 6a_1$, et $a_4 = 5a_3 - 6a_2$.

c) Montrer que $a_n = 5a_{n-1} - 6a_{n-2}$ pour tous les entiers n avec $n \geq 2$.

12. Montrer que la séquence $\{a_n\}$ est une solution de la récurrence relation $a_n = -3a_{n-1} + 4a_{n-2}$ si

a) $a_n = 0$.　　**b)** $a_n = 1$.

c) $a_n = (-4)^n$.　　**d)** $a_n = 2(-4)^n + 3$.

13. La séquence $\{a_n\}$ est-elle une solution de la relation de récurrence $a_n = 8a_{n-1} - 16a_{n-2}$ si

a) $a_n = 0$?　　**b)** $a_n = 1$?

c) $a_n = 2^n$?　　**d)** $a_n = 4^n$?

e) $a_n = n4^n$?　　**f)** $a_n = 2, 4^n + 3n4^n$?

g) $a_n = (-4)^n$?　　**h)** $a_n = n^2 4^n$?

14. Pour chacune de ces séquences trouver une relation de récurrence satisfait de cette séquence. (Les réponses ne sont pas uniques car il y a une infinité de récidives différentes relations satisfaites par n'importe quelle séquence.)

a) $a_n = 3$　　**b)** $a_n = 2n$

c) $a_n = 2n + 3$　　**d)** $a_n = 5^n$

e) $a_n = n^2$　　**f)** $a_n = n^2 + n$

g) $a_n = n + (-1)^n$　　**h)** $a_n = n!$

15. Montrer que la séquence $\{a_n\}$ est une solution de la récurrence relation $a_n = a_{n-1} + 2a_{n-2} + 2n - 9$ si

a) $a_n = -n + 2$.

b) $a_n = 5(-1)^n - n + 2$.

a) $a_n = 3a_{n-1}$, $a_0 = 2$

b) $a_n = a_{n-1} + 2$, $a_0 = 3$

c) $a_n = a_{n-1} + n$, $a_0 = 1$

d) $a_n = a_{n-1} + 2n + 3$, $a_0 = 4$

e) $a_n = 2a_{n-1} - 1$, $a_0 = 1$

f) $a_n = 3a_{n-1} + 1$, $a_0 = 1$

g) $a_n = na_{n-1}$, $a_0 = 5$

h) $a_n = 2na_{n-1}$, $a_0 = 1$

18. Une personne dépose 1 000 $ dans un compte qui rapporte 9% intérêts composés annuellement.

a) Établissez une relation de récurrence pour le montant de compter à la fin de *n* années.

b) Trouvez une formule explicite pour le montant dans le compte à la fin de *n* années.

c) Combien d'argent le compte contiendra-t-il après 100 ans?

19. Supposons que le nombre de bactéries dans une colonie triple Toutes les heures.

a) Établir une relation de récurrence pour le nombre de bactéries après *n* heures se sont écoulées.

b) Si 100 bactéries sont utilisées pour commencer une nouvelle colonie, comment de bactéries dans la colonie dans 10 heures?

20. Supposons que la population mondiale en 2010 était de 6,9 milliards et croît au rythme de 1,1% par an.

a) Etablir une relation de récurrence pour la population de la monde *n* ans après 2010.

b) Trouvez une formule explicite pour la population de la monde *n* ans après 2010.

c) Quelle sera la population mondiale en 2030?

21. Une usine fabrique des voitures de sport personnalisées à un rythme croissant. Le premier mois, une seule voiture est fabriquée, le deuxième mois deux voitures sont faites, et ainsi de suite, avec *n* voitures fabriquées en le *n* ème mois.

a) Etablir une relation de récurrence pour le nombre de voitures produite dans les *n* premiers mois par cette usine.

b) Combien de voitures sont produites la première année?

c) Trouvez une formule explicite pour le nombre de voitures dans les *n* premiers mois par cette usine.

22. Un employé a rejoint une entreprise en 2009 avec un salaire de 50 000 $. Chaque année, cet employé reçoit un augmentation de 1000 $ plus 5% du salaire de l'année précédente.

a) Etablir une relation de récurrence pour le salaire de cet employé *n* années après 2009.

b) Quel sera le salaire de cet employé en 2017?

c) Trouver une formule explicite pour le salaire de cet employé *n* années après 2009.

23. Trouver une relation de récurrence pour le solde $B(k)$ dû à la fin de *k* mois sur un prêt de 5000 $ au taux de 7% si un paiement de 100 $ est effectué chaque mois. [*Indice:* Exappuyez sur $B(k)$ en termes de $B(k-1)$; l'intérêt mensuel est $(0,07/12)\,B(k-1)$.]

24. a) Trouver une relation de récurrence pour le solde $B(k)$ dû à la fin de *k* mois sur un prêt au taux de *r* si un paiement *P* est effectué sur le prêt chaque mois. [*Astuce:* Express $B(k)$ en termes de $B(k-1)$ et notons que la valeur mensuelle le taux d'intérêt est de $r/12$.]

b) Déterminer quel devrait être le versement mensuel *P* que le prêt est remboursé après *T* mois.

25. Pour chacune de ces listes d'entiers, fournissez une formule simple formule ou règle qui génère les termes d'une séquence entière séquence qui commence par la liste donnée. En supposant que votre la formule ou la règle est correcte, déterminez les trois termes suivants de la séquence.

a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, ...

b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, ...

c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, ...

d) 3, 6, 12, 24, 48, 96, 192, ...

e) 15, 8, 1, −6, −13, −20, −27, ...

f) 3, 5, 8, 12, 17, 23, 30, 38, 47, ...

g) 2, 16, 54, 128, 250, 432, 686, ...

h) 2, 3, 7, 25, 121, 721, 5041, 40321, ...

30. Quelles sont les valeurs de ces sommes, où $S = \{1, 3, 5, 7\}$?

une) $\sum_{j \in S} j$　　**b)** $\sum_{j \in S} j^2$

c) $\sum_{j \in S} (1/j)$　　**ré)** $\sum_{j \in S} 1$

31. Quelle est la valeur de chacune de ces sommes d'une progression géométrique?

une) $\sum_{j=0}^{8} 3 \cdot 2^j$　　**b)** $\sum_{j=1}^{8} 2^j$

c) $\sum_{j=2}^{8} (-3)^j$　　**ré)** $\sum_{j=0}^{8} 2 \cdot (-3)^j$

32. Trouvez la valeur de chacune de ces sommes.

une) $\sum_{j=0}^{8} (1 + (-1)^j)$　　**b)** $\sum_{j=0}^{8} (3^j - 2^j)$

c) $\sum_{j=0}^{8} (2 \cdot 3^j + 3 \cdot 2^j)$　　**ré)** $\sum_{j=0}^{8} (2^{j+1} - 2^j)$

33. Calculez chacune de ces doubles sommes.

une) $\sum_{i=1}^{2} \sum_{j=1}^{3} (i + j)$　　**b)** $\sum_{i=0}^{2} \sum_{j=0}^{3} (2i + 3j)$

c) $\sum_{i=1}^{3} \sum_{j=0}^{2} je$　　**ré)** $\sum_{i=0}^{2} \sum_{j=1}^{3} ij$

34. Calculez chacune de ces doubles sommes.

une) $\sum_{i=1}^{3} \sum_{j=1}^{2} (i - j)$　　**b)** $\sum_{i=0}^{3} \sum_{j=0}^{2} (3i + 2j)$

c) $\sum_{i=1}^{3} \sum_{j=0}^{2} j$　　**ré)** $\sum_{i=0}^{2} \sum_{j=0}^{3} i^2 j^3$

$\sum_n$

26. Pour chacune de ces listes d’entiers, fournissez une formule simple formule ou règle qui génère les termes d'une séquence entière séquence qui commence par la liste donnée. En supposant que votre la formule ou la règle est correcte, déterminez les trois termes suivants de la séquence.

a) 3 , 6 , 11 , 18 , 27 , 38 , 51 , 66 , 83 , 102 , ...

b) 7 , 11 , 15 , 19 , 23 , 27 , 31 , 35 , 39 , 43 , ...

c) 1 , 10 , 11 , 100 , 101 , 110 , 111 , 1000 , 1001, 1010 , 1011 , ...

d) 1 , 2 , 2 , 2 , 3 , 3 , 3 , 3 , 3 , 5 , 5 , 5 , 5 , 5 , 5 , 5 , ...

e) 0 , 2 , 8 , 26 , 80 , 242 , 728 , 2186 , 6560 , 19682 , ...

f) 1 , 3 , 15 , 105 , 945 , 10395 , 135135 , 2027025, 34459425 , ...

g) 1 , 0 , 0 , 1 , 1 , 1 , 0 , 0 , 0 , 0 , 1 , 1 , 1 , 1 , 1 , ...

h) 2 , 4 , 16 , 256 , 65536 , 4294967296 , ...

** **27.** Montrer que si a_n désigne le n ème entier positif qui n'est pas un carré parfait, alors $a_n = n + \{\sqrt{n}\}$, où $\{x\}$ désigne l'entier le plus proche du nombre réel x .

* **28.** Soit a_n le n ième terme de la séquence 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6 , ..., construit en incluant l'entier k exactement k fois. Montrer que $a_n = \lfloor \sqrt{2n} + \frac{1}{2} \rfloor$.

29. Quelles sont les valeurs de ces sommes?

une) $\sum_{k=1}^{5} (k+1)$ **b)** $\sum_{j=0}^{4} (-2)^j$

c) $\sum_{i=1}^{\text{dix}} 3$ **ré)** $\sum_{j=0}^{8} (2^{j+1} - 2^j)$

35. Spectacle cette $\sum_{j=1}^{n} (a_j - a_{j-1}) = a_n - a_0$, où $a_0, a_1, \ldots, a_n$ est une séquence de nombres réels. Ce type de somme est appelée **télescopique** .

36. Utilisez l'identité $1/(k(k+1)) = 1/k - 1/(k+1)$ et Exercice 35 pour calculer $\sum_{k=1}^{n} 1/(k(k+1))$.

37. Additionner les deux côtés de l'identité $k^2 - (k-1)^2 = 2k - 1$ de $k = 1$ à $k = n$ et utilisez l'exercice 35 pour trouver

a) une formule pour $\sum_{k=1}^{n} (2k-1)$ (la somme des n premiers nombres naturels impairs).

b) une formule pour $\sum_{k=1}^{n} k$.

* **38.** Utilisez la technique donnée dans l'exercice 35, avec le résultat de l'exercice 37b, pour dériver la formule $\sum_{k=1}^{n} k^2$ donné dans le tableau 2. [*Astuce* : Prenez $un_k = k^3$ dans le télescopique somme dans l'exercice 35.]

39. Trouver $\sum_{k=100}^{200} k$. (Utilisez le tableau 2.)

40. Trouver $\sum_{k=99}^{200} k^3$. (Utilisez le tableau 2.)

* **41.** Trouver une formule pour $\sum_{k=0}^{m} \lfloor \sqrt{k} \rfloor$, lorsque m est positif entier.

* **42.** Trouver une formule pour $\sum_{k=0}^{m} \lfloor \sqrt[3]{k} \rfloor$, lorsque m est positif entier.

Il existe également une notation spéciale pour les produits. Le produit de $a_m, a_{m+1}, \ldots, a_n$ est représenté par $\prod_{j=m}^{n} a_j$, lu comme le produit

uct de $j = m$ à $j = n$ d' un_j .

43. Quelles sont les valeurs des produits suivants?

une) $\prod_{i=0}^{10} i$ **b)** $\prod_{i=5}^{8} i$

c) $\prod_{i=1}^{100} (-1)^i$ **ré)** $\prod_{i=1}^{10} 2$

Rappelons que la valeur de la fonction factorielle à un teger n , noté n !, est le produit des entiers positifs de 1 à n , inclus. De plus, nous précisons que 0! = 1.

44. Express n ! en utilisant la notation du produit.

45. Trouver $\sum_{j=0}^{4} j!$.

46. Trouver $\prod_{j=0}^{4} j!$.

Cardinalité des ensembles

introduction

Dans la définition 4 de la section 2.1, nous avons défini la cardinalité d'un ensemble fini comme le nombre d'éléments dans l'ensemble. Nous utilisons les cardinalités des ensembles finis pour nous dire quand ils ont la même taille, ou quand l'un est plus grand que l'autre. Dans cette section, nous étendons cette notion à des ensembles infinis. Autrement dit, nous allons définir ce que cela signifie pour deux ensembles infinis d'avoir la même cardinalité, nous fournissant un moyen pour mesurer les tailles relatives d'ensembles infinis.

Nous serons particulièrement intéressés par les innombrables ensembles infinis, qui sont des ensembles avec le même cardinalité comme l'ensemble des entiers positifs. Nous établirons le résultat surprenant que l'ensemble des les nombres rationnels sont infiniment dénombrables. Nous fournirons également un exemple d'un ensemble indénombrable lorsque nous montrons que l'ensemble des nombres réels n'est pas dénombrable.

Les concepts développés dans cette section ont d'importantes applications en informatique. UNE la fonction est appelée non calculable si aucun programme informatique ne peut être écrit pour retrouver toutes ses valeurs, même avec un temps et une mémoire illimités. Nous utiliserons les concepts de cette section pour expliquer pourquoi des fonctions non calculables existent.

Nous définissons maintenant ce que signifie que deux ensembles ont la même taille, ou cardinalité. Dans la section 2.1, nous avons discuté de la cardinalité des ensembles finis et nous avons défini la taille, ou cardinalité, de ces ensemblesDans L’exercice 79 de la section 2.3 a montré qu’il existe une correspondance biunivoque entre tout deux ensembles finis avec le même nombre d'éléments. Nous utilisons cette observation pour étendre le concept de cardinalité à tous les ensembles, à la fois finis et infinis.

DÉFINITION 1 Les ensembles A et B ont la même *cardinalité* si et seulement s'il y a une correspondance biunivoque de A à B . Lorsque A et B ont la même cardinalité, nous écrivons $|A| = |B|$.

Pour les ensembles infinis, la définition de la cardinalité fournit une mesure relative des tailles de deux ensembles, plutôt qu'une mesure de la taille d'un ensemble particulier. Nous pouvons également définir ce que cela signifie pour un défini pour avoir une cardinalité plus petite qu'un autre ensemble.

DÉFINITION 2 S'il y a une fonction un à un de A à B , la cardinalité de A est inférieure ou identique à la cardinalité de B et nous écrivons $|A| \leq |B|$. De plus, lorsque $|A| \leq |B|$ et A et B ont cardinalité différente, nous disons que la cardinalité de A est inférieure à la cardinalité de B et nous écrire $|A| < |B|$.

Ensembles dénombrables

Nous allons maintenant diviser les ensembles infinis en deux groupes, ceux ayant la même cardinalité que l'ensemble de les nombres naturels et ceux avec une cardinalité différente.

1 2 3 4 5 6 sept 8 9 dix 11 12 ...

1 3 5 sept 9 11 13 15 17 19 21 23 ...

FIGURE 1 Une correspondance biunivoque entre Z $^{+}$ **et l'ensemble des impairs positifs Entiers.**

DÉFINITION 3 Un ensemble fini ou ayant la même cardinalité que l'ensemble d'entiers positifs est appelé *dénombrable.* Un ensemble qui n'est pas dénombrable est appelé *non dénombrable.* Lorsqu'un ensemble infini S est dénombrable, nous désignons la cardinalité de S par $\aleph_0$ (où $\aleph$ est aleph, la première lettre de l'alphabet hébreu). Nous écrivons $|S| = \aleph_0$ et disons que S a une cardinalité «aleph null».

Nous illustrons comment montrer qu'un ensemble est dénombrable dans l'exemple suivant.

EXEMPLE 1 Montrez que l'ensemble d'entiers positifs impairs est un ensemble dénombrable.

Solution: Pour montrer que l'ensemble des entiers positifs impairs est dénombrable, nous allons présenter un à un correspondance entre cet ensemble et l'ensemble d'entiers positifs. Considérez la fonction

$$f(n) = 2n - 1$$

de $\mathbf{Z}^{+}$ à l'ensemble des entiers positifs impairs. Nous montrons que f est une correspondance biunivoque par montrant qu'il est à la fois un à un et sur. Pour voir que c'est un à un, supposons que $f(n) = f(m)$. Alors $2n - 1 = 2m - 1$, donc $n = m$. Pour voir qu'il est sur, supposons que t est un positif impair entier. Alors t est 1 de moins qu'un entier pair $2k$, où k est un nombre naturel. Donc $t = 2k - 1 = f(k)$. Nous affichons cette correspondance biunivoque dans la figure 1. ▲

Un ensemble infini est dénombrable si et seulement s'il est possible de lister les éléments de l'ensemble dans un séquence (indexée par les entiers positifs). La raison en est qu'une correspondance biunivoque dence f de l'ensemble des entiers positifs à un ensemble S peut être exprimée en termes de séquence $a_1, a_2, \ldots, a_n, \ldots$, où $a_1 = f(1)$, $a_2 = f(2), \ldots, a_n = f(n), \ldots$

Vous pouvez toujours obtenir une chambre au Hilbert's Grand Hotel!

HILBERT'S GRAND HOTEL Nous décrivons maintenant un paradoxe qui montre que quelque chose d'impos- possible avec des ensembles finis peut être possible avec des ensembles infinis. Le célèbre mathématicien David Hilbert inventé la notion du **Grand Hôtel** , qui dispose d'un nombre infini de chambres, chacune occupé par un invité. Lorsqu'un nouveau client arrive dans un hôtel avec un nombre fini de chambres, et toutes les chambres sont occupées, ce client ne peut pas être logé sans expulser un invité actuel. Cependant, nous pouvons toujours accueillir un nouvel invité au Grand Hôtel, même lorsque toutes les chambres sont déjà occupés, comme le montre l'exemple 2. Les exercices 5 et 8 vous demandent de montrer que nous pouvons accueillir un nombre fini de nouveaux invités et un nombre dénombrable de nouveaux invités, respectivement, au Grand Hôtel entièrement occupé.

DAVID HILBERT (1862-1943) Hilbert, né à Königsberg, la ville célèbre en mathématiques pour ses sept ponts, était le fils d'un juge. Pendant son mandat à l'Université de Göttingen, de 1892 à 1930, il a fait de nombreuses contributions fondamentales à un large éventail de matières mathématiques. Il a presque toujours travaillé sur un domaine mathématiques à la fois, apportant des contributions importantes, puis passer à une nouvelle matière mathématique. Certaines zones dans lequel Hilbert a travaillé sont le calcul des variations, la géométrie, l'algèbre, la théorie des nombres, la logique et les mathématiques la physique. Outre ses nombreuses contributions originales exceptionnelles, Hilbert est connu pour sa célèbre liste de 23 problèmes difficiles. Il a décrit ces problèmes au Congrès international des mathématiciens de 1900, défi aux mathématiciens à la naissance du XXe siècle. Depuis ce temps, ils ont stimulé un énorme quantité et variété de recherches. Bien que bon nombre de ces problèmes soient maintenant résolus, plusieurs restent ouverts, y compris l'hypothèse de Riemann, qui fait partie du problème 8 sur la liste de Hilbert. Hilbert est également l'auteur de plusieurs manuels de théorie des nombres et de géométrie.

. . .

. . .

8 . . .

sept

6

5

4

3

2

1

Hilbert's Grandiose Hôtel

Prenez la chambre 1, tous les autres descendre d'une pièce

Directeur

Nouvel invité

FIGURE 2 Un nouvel invité arrive au Hilbert's Grand Hotel.

EXEMPLE 2 Comment pouvons-nous accueillir un nouveau client arrivant au Grand Hôtel entièrement occupé sans supprimer l'un des invités actuels?

Solution: les chambres du Grand Hotel étant dénombrables, nous pouvons les répertorier en tant que chambre 1, Salle 2, salle 3, etc. Lorsqu'un nouveau client arrive, nous le transférons dans la chambre 1 vers la chambre 2, l'invité de la salle 2 à la salle 3, et en général, l'invité de la salle n à la salle n + 1, pour tous entiers positifs n . Cela libère la salle 1, que nous attribuons au nouvel invité, et tous les les clients ont encore des chambres. Nous illustrons cette situation dans la figure 2. ▲

Lorsqu'il y a un nombre fini de chambres dans un hôtel, la notion que toutes les chambres sont occupées est équivalent à l'idée qu'aucun nouvel invité ne peut être accueilli. Cependant, le paradoxe de Hilbert du Grand Hôtel peut s'expliquer en notant que cette équivalence ne tient plus lorsqu'il y a sont infiniment de place.

EXEMPLES D'ENSEMBLES COMPTABLES ET NON COMPTABLES Nous allons maintenant montrer que cer-certains ensembles de nombres sont dénombrables. Nous commençons par l'ensemble de tous les entiers. Notez que nous pouvons montrer que l'ensemble de tous les entiers est dénombrable en répertoriant ses membres.

EXEMPLE 3 Montrez que l'ensemble de tous les entiers est dénombrable.

Solution: Nous pouvons répertorier tous les entiers d'une séquence en commençant par 0 et en alternant entre positifs et négatifs des nombres entiers: 0 , 1 , -1 , 2 , -2 , ... Alternativement, nous pourrions trouver un tête-à-tête correspondance entre l'ensemble des entiers positifs et l'ensemble de tous les entiers. Nous laissons au lecteur pour montrer que la fonction $f(n) = n / 2$ lorsque n est pair et $f(n) = -(n - 1) / 2$ lorsque n est étrange est une telle fonction. Par conséquent, l'ensemble de tous les entiers est dénombrable. ▲

Il n'est pas surprenant que l'ensemble des entiers impairs et l'ensemble de tous les entiers soient tous deux dénombrables ensembles (comme illustré dans les exemples 1 et 3). Beaucoup de gens sont étonnés d'apprendre que l'ensemble des les nombres sont dénombrables, comme le montre l'exemple 4.

EXEMPLE 4 Montrer que l'ensemble des nombres rationnels positifs est dénombrable.

Solution: Il peut sembler surprenant que l'ensemble des nombres rationnels positifs soit dénombrable, mais nous montrera comment nous pouvons lister les nombres rationnels positifs comme une séquence $r_1, r_2, \ldots, r_n, \ldots$. Tout d'abord, notons que chaque nombre rationnel positif est le quotient p / q de deux entiers positifs. nous pouvons

Termes non encerclés ne sont pas répertoriés parce qu'ils répéter précédemment termes énumérés

$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{5}{1}$	...
$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$	...
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	$\frac{5}{3}$	...
$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{5}{4}$	...
$\frac{1}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{5}{5}$	...
...	...	...	...	...	

FIGURE 3 Les nombres rationnels positifs sont dénombrables.

organiser les nombres rationnels positifs en listant ceux avec le dénominateur $q = 1$ dans la première ligne, ceux dont le dénominateur $q = 2$ dans la deuxième ligne, et ainsi de suite, comme illustré à la figure 3.

La clé pour lister les nombres rationnels dans une séquence est de lister d'abord le rationnel positif nombres p / q avec $p + q = 2$, suivis de ceux avec $p + q = 3$, suivis de ceux avec $p + q = 4$, et ainsi de suite, en suivant le chemin indiqué dans la figure 3. Chaque fois que nous rencontrons un nombre p / q qui est déjà répertorié, nous ne le répertorions pas à nouveau. Par exemple, lorsque nous arrivons à $2 / 2 = 1$ nous ne liste pas parce que nous avons déjà mentionnées $1 / 1 = 1$. Les conditions initiales dans la liste des positifs des nombres rationnels , nous avons construit sont $1, 1 / 2, 2, 3, 1 / 3, 1 / 4, 2 / 3, 3 / 2, 4, 5$, et ainsi de suite. Celles-ci les chiffres sont encerclés; les chiffres non encerclés dans la liste sont ceux que nous laissons de côté parce que ils sont déjà répertoriés. Parce que tous les nombres rationnels positifs sont répertoriés une fois, comme le lecteur peut vérifier, nous avons montré que l'ensemble des nombres rationnels positifs est dénombrable. ▲

Un ensemble indénombrable

Tous les ensembles infinis n'ont pas la même taille!

Nous avons vu que l'ensemble des nombres rationnels positifs est un ensemble dénombrable. Avons-nous une promesse candidat pour un ensemble innombrable? Le premier endroit que nous pourrions regarder est l'ensemble des nombres réels. Dans Exemple 5, nous utilisons une méthode de preuve importante, introduite en 1879 par Georg Cantor et connue comme **argument de diagonalisation de Cantor** , pour prouver que l'ensemble des nombres réels n'est pas dénombrable. Cette méthode de preuve est largement utilisée en logique mathématique et en théorie du calcul.

EXEMPLE 5 Montrez que l'ensemble des nombres réels est un ensemble indénombrable.

Solution: pour montrer que l'ensemble des nombres réels est indénombrable, nous supposons que l'ensemble des réels les chiffres sont dénombrables et arrivent à une contradiction. Ensuite, le sous-ensemble de tous les nombres réels entre 0 et 1 serait également dénombrable (car tout sous-ensemble d'un ensemble dénombrable est également dénombrable; voir exercice 16). Dans cette hypothèse, les nombres réels entre 0 et 1 peuvent être énumérés dans un ordre, disons, $r_1, r_2, r_3, \ldots$. Que la représentation décimale de ces nombres réels soit

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\ldots$$
$$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\ldots$$
$$r_3 = 0.d_{31}d_{32}d_{33}d_{34}\ldots$$
$$r_4 = 0.d_{41}d_{42}d_{43}d_{44}\ldots$$
$$\ldots$$

où $d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. (Par exemple, si $r_1 = 0.23794102\ldots$, nous avons ; $d_{11} = 2$, $d_{12} = 3$, $d_{13} = 7$, etc.). Ensuite, formez un nouveau nombre réel avec une expansion décimale

$r = 0.d_1 d_2 d_3 d_4 \ldots$, où les chiffres décimaux sont déterminés par la règle suivante:

$$d_i = \begin{cases} 4 \text{ si } d_{ii} = 4 \\ 5 \text{ si } d_{ii} = 4. \end{cases}$$

(A titre d'exemple, supposons que $r_1 = 0.23794102\ldots$, $r_2 = 0.44590138\ldots$, $r_3 = 0.09118764\ldots$, $r_4 = 0.80553900\ldots$, et ainsi de suite. On a alors $r = 0.d_1 d_2 d_3 d_4 \ldots = 0.4544\ldots$, où $d_1 = 4$ car $d_{11} = 4$, $d_2 = 5$ car $d_{22} = 4$, $d_3 = 4$ car $d_{33} = 4$, $d_4 = 4$ car $d_{44} = 4$, etc.)

Un nombre avec une décimale expansion qui se termine a une deuxième décimale expansion se terminant par un séquence infinie de 9s car $1 = 0.999\ldots$

Chaque nombre réel a une expansion décimale unique (lorsque la possibilité que l'extension a une extrémité qui se compose entièrement du chiffre 9 est exclu). Par conséquent, le nombre réel r n'est pas égal à l'un des r_1, r_2, ... car l'expansion décimale de r diffère de l'expansion décimale de r_i à la i ème place à droite de la virgule décimale, pour chaque i.

Parce qu'il y a un vrai nombre r entre 0 et 1 qui n'est pas dans la liste, l'hypothèse que tous les vrais nombres entre 0 et 1 pouvant être listés doivent être faux. Par conséquent, tous les vrais nombres entre 0 et 1 ne peut pas être répertorié, donc l'ensemble des nombres réels entre 0 et 1 est indénombrable. Tout ensemble avec un sous-ensemble indénombrable est indénombrable (voir exercice 15). Par conséquent, l'ensemble des nombres réels est innombrable. ▲

RÉSULTATS SUR LA CARDINALITÉ Nous allons maintenant discuter de quelques résultats sur la cardinalité d'ensembles. Premièrement, nous prouverons que l'union de deux ensembles dénombrables est également dénombrable.

THÉORÈME 1 Si A et B sont des ensembles dénombrables, alors $A \cup B$ est également dénombrable.

Cette preuve utilise WLOG et les cas.

Preuve: Supposons que A et B sont tous deux des ensembles dénombrables. Sans perte de généralité, on peut supposer que A et B sont disjoints. (S'ils ne le sont pas, on peut remplacer B par $B - A$, car $A \cap (B - A) = \emptyset$ et $A \cup (B - A) = A \cup B$.) De plus, sans perte de généralité, si l'un des deux ensembles est infiniment infini et autres finis, nous pouvons supposer que B est celui qui est fini.

Il y a trois cas à considérer: (i) A et B sont tous deux finis, (ii) A est infini et B est fini, et (iii) A et B sont tous deux infiniment dénombrables.

Cas (i): Notez que lorsque A et B sont finis, $A \cup B$ est également fini, et donc comptable.

Cas (ii): Parce que A est infiniment dénombrable, ses éléments peuvent être répertoriés dans une séquence infinie $a_1, a_2, a_3, \ldots, a_n, \ldots$ et parce que B est fini, ses termes peuvent être listés comme $b_1, b_2, \ldots, b_m$ pour un entier positif m. On peut lister les éléments de $A \cup B$ comme $b_1, b_2, \ldots, b_m, a_1, a_2, a_3, \ldots, un_n, \ldots$. Cela signifie que $A \cup B$ est infiniment comptable.

Cas (iii): Parce que A et B sont infiniment dénombrables, nous pouvons lister leurs éléments comme un_1, $a_2, a_3, \ldots, a_n, \ldots$ et $b_1, b_2, b_3, \ldots, b_n, \ldots$, respectivement. En alternant les termes de ces deux séquences on peut lister les éléments de $A \cup B$ dans la séquence infinie $a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n, \ldots$. Cela signifie que $A \cup B$ doit être infiniment dénombrable.

Nous avons terminé la preuve, car nous avons montré que $A \cup B$ est dénombrable dans les trois cas.

En raison de son importance, nous énonçons maintenant un théorème clé dans l'étude de la cardinalité.

THÉORÈME 2 **THÉORÈME DE SCHRÖDER-BERNSTEIN** Si A et B sont des ensembles avec $|A| \leq |B|$ et $|B| \leq |A|$, puis $|A| = |B|$. En d'autres termes, s'il existe des fonctions *biunivoque* f de A à B et g de B à A, alors il y a un-à-un entre A et B.

Parce que le théorème 2 semble être assez simple, nous pouvons nous attendre à ce qu'il ait un preuve. Cependant, même si cela peut être prouvé sans utiliser de mathématiques avancées, aucune la preuve est facile à expliquer. Par conséquent, nous omettons ici une preuve. Nous renvoyons le lecteur intéressé à [AiZiHo09] et [Ve06] pour une preuve. Ce résultat est appelé le théorème de Schröder-Bernstein après Ernst Schröder qui en a publié une preuve imparfaite en 1898 et Felix Bernstein, élève de Georg Cantor, qui a présenté une preuve en 1897. Cependant, une preuve de ce théorème a été trouvée dans les notes de Richard Dedekind datées de 1887. Dedekind était un mathématicien allemand qui a fait contributions importantes aux fondements des mathématiques, de l'algèbre abstraite et de la théorie des nombres.

Nous illustrons l'utilisation du théorème 2 avec un exemple.

EXEMPLE 6 Montrer que le $|(0,1)| = |(0,1]|$.

Solution: il n'est pas du tout évident de trouver une correspondance biunivoque entre $(0,1)$ et $(0,1]$ pour montrer que $|(0,1)| = |(0,1]|$. Heureusement, nous pouvons utiliser le théorème de Schröder-Bernstein au lieu. Trouver une fonction un à un de $(0,1)$ à $(0,1]$ est simple. Parce que $(0,1) \subset (0,1]$, $f(x) = x$ est une fonction biunivoque de $(0,1)$ à $(0,1]$. Trouver une fonction biunivoque à partir de $(0,1]$ à $(0,1)$ n'est pas non plus difficile. La fonction $g(x) = x/2$ est clairement biunivoque et mappe $(0,1]$ à $(0,1/2] \subset (0,1)$. Comme nous l'avons trouvé un-à-un à partir de fonctions $(0,1)$ à $(0,1]$ et de $(0,1]$ à $(0,1)$, le théorème de Schröder-Bernstein nous dit que $|(0,1)| = |(0,1]|$. ▲

FONCTIONS INCOMPUTABLES Nous allons maintenant décrire une application importante du concepts de cette section à l'informatique. En particulier, nous montrerons qu'il existe des fonctions dont les valeurs ne peuvent être calculées par aucun programme informatique.

DÉFINITION 4 Nous disons qu'une fonction est **calculable** s'il y a un programme informatique dans certains programmes langage qui trouve les valeurs de cette fonction. Si une fonction n'est pas calculable, nous disons qu'elle est **non calculable** .

Pour montrer qu'il existe des fonctions non calculables, nous devons établir deux résultats. Premièrement, nous besoin de montrer que l'ensemble de tous les programmes informatiques dans un langage de programmation particulier est dénombrable. Cela peut être prouvé en notant qu'un programme informatique dans une langue particulière peut être considéré comme une chaîne de caractères d'un alphabet fini (voir exercice 37). Ensuite, nous montrons qu'il existe de nombreuses fonctions différentes d'un ensemble infiniment dénombrable particulier à lui-même. En particulier, l'exercice 38 montre que l'ensemble des fonctions de l'ensemble des entiers positifs en soi est innombrable. Ceci est une conséquence de l'indénombrabilité des nombres réels entre 0 et 1 (voir l'exemple 5). L'association de ces deux résultats (exercice 39) montre qu'il existe fonctions non calculables.

L'HYPOTHÈSE CONTINUE Nous concluons cette section par une brève discussion d'un célèbre question ouverte sur la cardinalité. On peut montrer que l'ensemble de puissance de $\mathbf{Z}^+$ et l'ensemble des nombres réels **R** ont la même cardinalité (voir exercice 38). En d'autres termes, nous savons que $|P(\mathbf{Z}^+)| = |\mathbf{R}| = \mathfrak{c}$, où $\mathfrak{c}$ désigne la cardinalité de l'ensemble des nombres réels.

Un théorème important de Cantor (exercice 40) déclare que la cardinalité d'un ensemble est toujours inférieure que la cardinalité de son pouvoir. Par conséquent, $|\mathbf{Z}^+| < |P(\mathbf{Z}^+)|$. Nous pouvons réécrire ceci comme $\aleph_0 < 2^{\aleph_0}$, en utilisant la notation $2^{|S|}$ pour désigner la cardinalité de l'ensemble d'alimentation de l'ensemble S. Notez également que relation $|P(\mathbf{Z}^+)| = |\mathbf{R}|$ peut être exprimé comme $2^{\aleph_0} = \mathfrak{c}$.

Cela nous amène à la fameuse **hypothèse du continuum** , qui affirme qu'il n'y a pas de cardinal nombre X entre $\aleph_0$ et $\mathfrak{c}$. En d'autres termes, l'hypothèse du continuum indique qu'il n'y a pas d'ensemble A tel que $\aleph_0$, la cardinalité de l'ensemble des entiers positifs, est inférieure à $|A|$ et $|A|$ est inférieur à $\mathfrak{c}$, la cardinalité de l'ensemble des nombres réels. On peut montrer que le plus petit cardinal infini les nombres forment une séquence infinie $\aleph_0 < \aleph_1 < \aleph_2 < \cdots$. Si nous supposons que le continuum l'hypothèse est vraie, il s'ensuit que $\mathfrak{c} = \aleph_1$, de sorte que $2^{\aleph_0} = \aleph_1$.

c est la minuscule Fraktur c.

L'hypothèse du continuum a été énoncée par Cantor en 1877. Il a travaillé sans succès pour prouver il, devenant extrêmement consterné qu'il ne pouvait pas. En 1900, régler l'hypothèse du continuum était considéré comme l'un des problèmes non résolus les plus importants en mathématiques. C'était le premier problème posé par David Hilbert dans sa célèbre liste de 1900 de problèmes ouverts en mathématiques.

L'hypothèse du continuum reste une question ouverte et reste un domaine de recherche active. Cependant, il a été démontré qu'il ne peut être ni prouvé ni réfuté dans le cadre de la norme axiomes théoriques en mathématiques modernes, les axiomes de Zermelo-Fraenkel. Le Zermelo-Fraenkel les axiomes ont été formulés pour éviter les paradoxes de la théorie naïve des ensembles, comme le paradoxe de Russell, mais il y a beaucoup de controverse quant à leur remplacement par un autre ensemble d'axiomes pour définir la théorie.

Des exercices

1. Déterminez si chacun de ces ensembles est fini, dénombrable infini ou innombrable. Pour ceux qui sont fini, présentent une correspondance biunivoque entre les ensemble d'entiers positifs et cet ensemble.

a) les entiers négatifs
b) les entiers pairs
c) les nombres entiers inférieurs à 100
d) les nombres réels entre 0 et $\frac{1}{2}$
e) les entiers positifs inférieurs à 1 000 000 000
f) les entiers multiples de 7

2. Déterminez si chacun de ces ensembles est fini, dénombrable infini ou innombrable. Pour ceux qui sont fini, présentent une correspondance biunivoque entre les ensemble d'entiers positifs et cet ensemble.

a) les entiers supérieurs à 10
b) les entiers négatifs impairs
c) les nombres entiers ayant une valeur absolue inférieure à 1 , 000 , 000
d) les nombres réels entre 0 et 2
e) l'ensemble $A \times \mathbf{Z}^+$ où $A = \{2 , 3\}$
f) les entiers multiples de 10

3. Déterminez si chacun de ces ensembles est dénombrable ou non. dénombrable. Pour ceux qui sont infiniment dénombrables, présentez une correspondance biunivoque entre l'ensemble des positifs entiers et cet ensemble.

a) toutes les chaînes de bits ne contenant pas le bit 0
b) tous les nombres rationnels positifs qui ne peuvent pas être écrits avec des dénominateurs inférieurs à 4
c) les nombres réels ne contenant pas 0 dans leur décimale représentation
d) les nombres réels ne contenant qu'un nombre fini de 1s dans leur représentation décimale

4. Déterminez si chacun de ces ensembles est dénombrable ou non. dénombrable. Pour ceux qui sont infiniment dénombrables, présentez une correspondance biunivoque entre l'ensemble des positifs entiers et cet ensemble.

a) entiers non divisibles par 3
b) entiers divisibles par 5 mais pas par 7
c) les nombres réels avec des représentations décimales con- composé de tous les 1
d) les nombres réels avec des représentations décimales de tous 1s ou 9s

5. Montrez qu'un groupe limité d'invités arrivant au Hilbert's le Grand Hôtel entièrement occupé peut recevoir des chambres sans expulser tout invité actuel.

6. Supposons que le Grand Hôtel de Hilbert soit entièrement occupé, mais l'hôtel ferme toutes les chambres numérotées paires pour nance. Montrez que tous les clients peuvent rester à l'hôtel.

7. Supposons que le Hilbert's Grand Hotel soit entièrement occupé le le jour où l'hôtel s'agrandit pour devenir un deuxième bâtiment qui contient un nombre infiniment infini de chambres. Montre CA les invités actuels peuvent être répartis pour remplir chaque pièce de les deux bâtiments de l'hôtel.

8. Montrer qu'un nombre infiniment infini d'invités sont arrivés au Grand Hôtel entièrement occupé de Hilbert peut être chambres sans expulser aucun invité actuel.

∗ **9.** Supposons qu'un nombre infiniment infini de bus, chacun contenant un nombre infiniment d'invités, arriver au Grand Hôtel entièrement occupé de Hilbert. Montrez que tous les les clients arrivant peuvent être logés sans expulsion tout invité actuel.

10. Donnez un exemple de deux ensembles innombrables A et B tels que $A - B$ est

a) fini.
b) infiniment dénombrable.
c) innombrable.

11. Donnez un exemple de deux ensembles innombrables A et B tels que $A \cap B$ est

a) fini.
b) infiniment dénombrable.
c) innombrable.

12. Montrer que si A et B sont des ensembles et $A \subset B$ alors $|A| \leq |B|$.

13. Expliquez pourquoi l'ensemble A est dénombrable si et seulement si $|A| \leq |\mathbf{Z}^+|$.

14. Montrez que si A et B sont des ensembles avec la même cardinalité, alors $|A| \leq |B|$ et $|B| \leq |A|$.

15. Montrez que si A et B sont des ensembles, A est indénombrable et $A \subseteq B$, alors B est indénombrable.

16. Montrer qu'un sous-ensemble d'un ensemble dénombrable est également dénombrable.

17. Si A est un ensemble dénombrable et B est un ensemble dénombrable, doit $A - B$ est-il innombrable?

18. Montrez que si A et B sont des ensembles $|A| = |B|$, puis $|P(A)| = |P(B)|$.

19. Montrez que si A , B , C et D sont des ensembles avec $|A| = |B|$ et $|C| = |D|$, puis $|A \times C| = |B \times D|$.

20. Montrez que si $|A| = |B|$ et $|B| = |C|$, puis $|A| = |C|$.

21. Montrer que si A , B et C sont des ensembles tels que $|A| \leq |B|$ et $|B| \leq |C|$, puis $|A| \leq |C|$.

22. Supposons que A est un ensemble dénombrable. Montrer que l'ensemble B est aussi dénombrable si une fonction sur f de A à B .

23. Montrer que si A est un ensemble infini, alors il contient un compte- sous-ensemble bien infini.

24. Montrer qu'il n'y a pas d'ensemble A infini tel que $|A| < |\mathbf{Z}^+| = \aleph_0$.

25. Prouver que s'il est possible d'étiqueter chaque élément d'un ensemble infini S avec une chaîne finie de caractères du clavier, à partir d'une liste de caractères finis, où il n'y a pas deux éléments de S ont la même étiquette, alors S est un ensemble infiniment dénombrable.

26. Utilisez l'exercice 25 pour fournir une preuve différente de celle dans le texte que l'ensemble des nombres rationnels est dénombrable. [*Astuce:* Montrez que vous pouvez exprimer un nombre rationnel comme chaîne de chiffres avec une barre oblique et éventuellement un signe moins.]

∗ **27.** Montrer que l'union d'un nombre dénombrable de dénombrable ensembles est dénombrable.

28. Montrer que l'ensemble $\mathbf{Z}^+ \times \mathbf{Z}^+$ est dénombrable.

∗ **29.** Montrez que l'ensemble de toutes les chaînes de bits finis est dénombrable.

∗ **30.** Montrer que l'ensemble des nombres réels qui sont des solutions de équations quadratiques $ax^2 + bx + c = 0$, où a, b et c

33. Utilisez le théorème de Schröder-Bernstein pour montrer que $(0 , 1)$ et $[0 , 1]$ ont la même cardinalité

34. Montrez que $(0 , 1)$ et $\mathbf{R}$ ont la même cardinalité. [*Indice:* Utilisez le théorème de Schröder-Bernstein.]

35. Montrer qu'il n'y a pas de correspondance individuelle de l'ensemble des entiers positifs à l'ensemble de puissance de l'ensemble de entiers positifs. [*Astuce:* Supposons qu'il existe un tel- correspondance individuelle. Représenter un sous-ensemble de l'ensemble de entiers positifs sous forme de chaîne de bits infinis avec i ème bit 1 si i appartient au sous-ensemble et 0 sinon. Supposons que vous peut répertorier ces chaînes infinies dans une séquence indexée par le entiers positifs. Construire une nouvelle chaîne de bits avec son i ème bit égal au complément du i ème bit de la i ème chaîne dans la liste. Montrer que cette nouvelle chaîne de bits ne peut pas apparaître dans la liste.]

∗ **36.** Montrer qu'il existe une correspondance biunivoque avec le ensemble de sous-ensembles des entiers positifs au nombre réel défini entre 0 et 1. Utilisez ce résultat et les exercices 34 et 35 pour conclure que $\aleph_0 < |P(\mathbf{Z}^+)| = |\mathbf{R}|$. [*Indice:* regardez la première partie de l'indice de l'exercice 35.]

∗ **37.** Montrer que l'ensemble de tous les programmes informatiques d'un ular langage de programmation est dénombrable. [*Indice:* une com- programme informatique écrit dans un langage de programmation peut être considéré comme une chaîne de symboles d'un alphabet fini.]

∗ **38.** Montrer que l'ensemble des fonctions de l'intégrale positive gers à l'ensemble $\{0 , 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9\}$ est indénombrable. [*Conseil:* commencez par établir une correspondance biunivoque entre l'ensemble des nombres réels compris entre 0 et 1 et un sous-ensemble de ces fonctions. Pour ce faire, en associant au nombre réel sont des entiers, est dénombrable.

∗ **31.** Montrez que $\mathbf{Z}^+ \times \mathbf{Z}^+$ est dénombrable en montrant que la fonction polynomiale $f : \mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ avec $f(m, n) = (m + n - 2)(m + n - 1)/2 + m$ est un à un et sur.

∗ **32.** Montrez que lorsque vous remplacez $(3n + 1)^2$ pour chaque occurrence de n et $(3m + 1)^2$ pour chaque occurrence de m dans le côté droit de la formule de la fonction $f(m, n)$ à l'exercice 31, vous obtenez une fonction polynomiale biunivoque tion $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$. C'est une question ouverte s'il y a une fonction one-to-one polynôme $\mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}$.

$0.d_1 d_2 \ldots d_n \ldots$ la fonction f avec $f(n) = d_n$.]

∗ **39.** On dit qu'une fonction est **calculable** s'il y a un com- programme informatique qui trouve les valeurs de cette fonction. Utilisation Les exercices 37 et 38 montrent qu'il existe des fonctions qui ne sont pas calculables.

∗ **40.** Montrer que si S est un ensemble, alors il n'existe pas de sur la fonction f de S à $P(S)$, l'ensemble de puissance S. Con- comprendre que $|S| < |P(S)|$. Ce résultat est connu sous le nom de **Cantor théorème**. [*Indice:* supposons qu'une telle fonction f existe. Laisser $T = \{ s \in S \mid s \in f(s) \}$ et montrer qu'aucun élément s ne peut existent pour lesquels $f(s) = T$.]

Matrices

introduction

Les matrices sont utilisées dans les mathématiques discrètes pour exprimer les relations entre les éléments en ensembles. Dans les chapitres suivants, nous utiliserons des matrices dans une grande variété de modèles.Par exemple, des matrices seront utilisées dans des modèles de réseaux de communication et de systèmes de transport.Beaucoup des algorithmes seront développés utilisant ces modèles matriciels.Cette section passe en revue l'arithmétique matricielle qui sera utilisé dans ces algorithmes.

DÉFINITION 1 Une *matrice* est un tableau rectangulaire de nombres. Une matrice avec m lignes et n colonnes est appelée une matrice $m \times n$. Le pluriel de matrice est *matrices.* Une matrice avec le même nombre de lignes comme colonnes est appelé *carré.* Deux matrices sont *égales* si elles ont le même nombre de lignes et le même nombre de colonnes et les entrées correspondantes dans chaque position sont égales.

EXEMPLE 1 La matrice $\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$ est une matrice 3×2. ▲

Nous introduisons maintenant une terminologie sur les matrices.Les lettres majuscules en gras seront utilisé pour représenter les matrices.

DÉFINITION 2 Soit m et n des entiers positifs et soit

$$\mathbf{A} = \begin{bmatrix} un_{11} & un_{12} & \ldots & a_{1n} \\ un_{21} & un_{22} & \ldots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & un_{m2} & \ldots & une_{mn} \end{bmatrix}.$$

La i ème *ligne* de **A** est la matrice $1 \times n$ $[a_{i1}, a_{i2}, \ldots, a_{in}]$. La j ème *colonne* de **A** est le $m \times 1$ matrice

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \cdot \\ \cdot \\ \cdot \\ un_{mj} \end{bmatrix}.$$

L' *élément* (i, j) e ou l' *entrée* de **A** est l'élément a_{ij}, c'est-à-dire le nombre sur la i e ligne et j ième colonne de **A**. Une notation abrégée pratique pour exprimer la matrice **A** consiste à écrire $\mathbf{A} = [a_{ij}]$, ce qui indique que **A** est la matrice avec son (i, j) e élément égal à a_{ij}.

Arithmétique matricielle

Les opérations de base de l'arithmétique matricielle seront maintenant discutées, en commençant par une définition de ajout de matrice.

DÉFINITION 3 Soit $\mathbf{A} = [a_{ij}]$ et $\mathbf{B} = [b_{ij}]$ des $m \times n$ matrices. La *somme* de $\mathbf{A}$ et $\mathbf{B}$, notée $\mathbf{A} + \mathbf{B}$, est la matrice $m \times n$ qui a $\mathit{un}_{ij} + b_{ij}$ comme (i, j) e élément. En d'autres termes, $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$.

La somme de deux matrices de même taille est obtenue en ajoutant des éléments dans le postes. Des matrices de tailles différentes ne peuvent pas être ajoutées, car la somme de deux matrices est définie uniquement lorsque les deux matrices ont le même nombre de lignes et le même nombre de colonnes.

EXEMPLE 2 Nous avons

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}.$$

▲

Nous discutons maintenant des produits matriciels. Un produit de deux matrices n'est défini que lorsque le nombre de colonnes dans la première matrice est égal au nombre de lignes de la deuxième matrice.

DÉFINITION 4 Soit $\mathbf{A}$ une matrice $m \times k$ et $\mathbf{B}$ une matrice $k \times n$. Le *produit* de $\mathbf{A}$ et $\mathbf{B}$, noté $\mathbf{AB}$, est la matrice $m \times n$ avec sa (i, j) ème entrée égale à la somme des produits des des éléments de la i ième ligne de $\mathbf{A}$ et de la j ième colonne de $\mathbf{B}$. En d'autres termes, si $\mathbf{AB} = [c_{ij}]$, alors

$$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{ik} b_{kj}.$$

Dans la figure 1, la ligne colorée de $\mathbf{A}$ et la colonne colorée de $\mathbf{B}$ sont utilisées pour calculer l'élément c_{ij} de $\mathbf{AB}$. Le produit de deux matrices n'est pas défini lorsque le nombre de colonnes dans la première matrice et le nombre de lignes dans la deuxième matrice ne sont pas les mêmes.

Nous donnons maintenant quelques exemples de produits matriciels.

EXEMPLE 3 Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \quad \text{et} \quad \mathbf{B} = \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix}.$$

Recherchez $\mathbf{AB}$ s'il est défini.

Solution: Parce que $\mathbf{A}$ est une matrice 4×3 et $\mathbf{B}$ est une matrice 3×2, le produit $\mathbf{AB}$ est défini et est une matrice 4×2. Pour trouver les éléments de $\mathbf{AB}$, les éléments correspondants des rangées de $\mathbf{A}$ et le les colonnes de $\mathbf{B}$ sont d'abord multipliées, puis ces produits sont ajoutés. Par exemple, l'élément dans la (3, 1) ème position de $\mathbf{AB}$ est la somme des produits des éléments correspondants du troisième ligne de $\mathbf{A}$ et la première colonne de $\mathbf{B}$; à savoir, $3 \cdot 2 + 1 \cdot 1 + 0 \cdot 3 = 7$. Lorsque tous les éléments de $\mathbf{AB}$ sont calculés, on voit que

$$\mathbf{AB} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}.$$

▲

La multiplication matricielle n'est *pas* commutative. Autrement dit, si $\mathbf{A}$ et $\mathbf{B}$ sont deux matrices, ce n'est pas nécessairement vrai que $\mathbf{AB}$ et $\mathbf{BA}$ sont les mêmes. En fait, il se peut que seul un de ces deux produits est défini. Par exemple, si $\mathbf{A}$ est 2×3 et $\mathbf{B}$ est 3×4, alors $\mathbf{AB}$ est défini et est 2×4; cependant $\mathbf{BA}$ n'est pas défini, car il est impossible de multiplier une matrice 3×4 et une matrice 2×3 matrice.

En général, supposons que $\mathbf{A}$ est une matrice $m \times n$ et $\mathbf{B}$ est une matrice $r \times s$. Alors $\mathbf{AB}$ est défini uniquement lorsque $n = r$ et $\mathbf{BA}$ n'est défini que lorsque $s = m$. De plus, même lorsque $\mathbf{AB}$ et $\mathbf{BA}$ sont

$$\begin{bmatrix} \mathit{un}_{11} & \mathit{un}_{12} & \ldots & \mathit{un}_{1k} \\ \mathit{un}_{21} & \mathit{un}_{22} & \ldots & \mathit{un}_{2k} \\ \cdots & \cdots & & \cdots \\ a_{i1} & a_{i2} & \ldots & \mathit{un}_{ik} \\ \cdots & \cdots & & \cdots \\ a_{m1} & \mathit{un}_{m2} & \ldots & \mathit{un}_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1j} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2j} & \ldots & b_{2n} \\ \cdots & \cdots & & \cdots & & \cdots \\ b_{k1} & b_{k2} & \ldots & b_{kj} & \ldots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \cdots & \cdots & c_{ij} & \cdots \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{bmatrix}$$

FIGURE 1 Le produit de $\mathbf{A} = [a_{ij}]$ et $\mathbf{B} = [b_{ij}]$.

tous deux définis, ils ne seront pas de la même taille sauf si $m = n = r = s$. Par conséquent, si **AB** et **BA** sont définis et ont la même taille, alors **A** et **B** doivent être carrés et de même taille.
De plus, même avec **A** et **B, les** deux matrices $n \times n$, **AB** et **BA** ne sont pas nécessairement égales, car L'exemple 4 le démontre.

EXEMPLE 4 Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \quad \text{et} \quad \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

Est-ce que **AB** = **BA?**

Solution: Nous constatons que

$$\mathbf{AB} = \begin{bmatrix} 3 & 2 \\ 5 & 3 \end{bmatrix} \quad \text{et} \quad \mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}.$$

Par conséquent, **AB** = **BA** . ▲

Transpose et pouvoirs des matrices

Nous introduisons maintenant une matrice importante avec des entrées qui sont des zéros et des uns.

DÉFINITION 5 La *matrice d'identité d'ordre n* est la matrice $n \times n$ $\mathbf{I}_n = [\delta_{ij}]$, où $\delta_{ij} = 1$ si $i = j$ et $\delta_{ij} = 0$ si $i = j$. Par conséquent

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

La multiplication d'une matrice par une matrice d'identité de taille appropriée ne change pas cette matrice. Dans autrement dit, lorsque **A** est une matrice $m \times n$, nous avons

$$\mathbf{AI}_n = \mathbf{I}_m\mathbf{A} = \mathbf{A}.$$

Les pouvoirs des matrices carrées peuvent être définis. Lorsque **A** est une matrice $n \times n$, nous avons

$$\mathbf{A}^0 = \mathbf{I}_n, \qquad \text{UNE} = \underbrace{\mathbf{AAA} \cdots \mathbf{A}}_{r \text{ fois}}.$$

L'opération d'interchanger les lignes et les colonnes d'une matrice carrée se pose dans de nombreux contextes.

DÉFINITION 6 Soit $\mathbf{A} = [a_{ij}]$ une matrice $m \times n$. La *transposition* de **A** , notée $\mathbf{A}^t$, est la matrice $n \times m$ obtenue en interchangeant les rangées et lescolonnes **A** . En d'autres termes, si $\mathbf{A}^t = [b_{ij}]$, alors $b_{ij} = a_{ji}$ pour $i = 1, 2, ..., n$ et $j = 1, 2, ..., m$.

EXEMPLE 5 La transposition de la matrice $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ est la matrice $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$. ▲

Les matrices qui ne changent pas lorsque leurs lignes et colonnes sont échangées sont souvent im-important.

DÉFINITION 7 Une matrice carrée **A** est dite *symétrique* si $\mathbf{A} = \mathbf{A}^t$. Ainsi $\mathbf{A} = [a_{ij}]$ est symétrique si $a_{ij} = a_{ji}$ pour tout i et j avec $1 \le i \le n$ et $1 \le j \le n$.

Notez qu'une matrice est symétrique si et seulement si elle est carrée et elle est symétrique par rapport à son diagonale principale (qui se compose d'entrées qui se trouvent dans la i ème ligne et la i ème colonne pour certains i). Cette la symétrie est affichée dans la figure 2.

EXEMPLE 6 La matrice $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ est symétrique. ▲

un $_{ji}$

a_{ij}

FIGURE 2 **A Matrice symétrique.**

Matrices zéro à un

Une matrice dont toutes les entrées sont 0 ou 1 est appelée **matrice zéro-un** . Matrices zéro-un sont souvent utilisés pour représenter des structures discrètes, comme nous le verrons dans les chapitres 9 et 10. Algorithmes l'utilisation de ces structures est basée sur l'arithmétique booléenne avec des matrices nulles.Cette arithmétique est basé sur les opérations booléennes ∧ et ∨, qui opèrent sur des paires de bits, définies par

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{si } b_1 = b_2 = 1 \\ 0 & \text{sinon,} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 & \text{si } b_1 = 1 \text{ ou } b_2 = 1 \\ 0 & \text{sinon.} \end{cases}$$

DÉFINITION 8 Soit $\mathbf{A} = [a_{ij}]$ et $\mathbf{B} = [b_{ij}]$ des $m \times n$ matrices zéro – un. Ensuite, la *jointure* de **A** et **B** est la matrice zéro – un avec (i, j) e entrée $a_{ij} \vee b_{ij}$. La jointure de **A** et **B** est noté $\mathbf{A} \vee \mathbf{B}$. le *La rencontre* de **A** et **B** est la matrice zéro-un avec (i, j) la troisième entrée $a_{ij} \wedge b_{ij}$. La rencontre de **A** et **B** est notée $\mathbf{A} \wedge \mathbf{B}$.

EXEMPLE 7 Trouver la jointure et la rencontre des matrices zéro-un

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Solution: Nous constatons que la jointure de **A** et **B** est

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

La rencontre de **A** et **B** est

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

▲

Nous définissons maintenant le **produit booléen** de deux matrices.

DÉFINITION 9 Soit $\mathbf{A} = [a_{ij}]$ une matrice $m \times k$ zéro – un et $\mathbf{B} = [b_{ij}]$ une matrice $k \times n$ zéro – un. alors le *produit booléen* de **A** et **B**, noté $\mathbf{A} \odot \mathbf{B}$, est la matrice $m \times n$ avec (i, j) e entrée c_{ij} où

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{ik} \wedge b_{kj}).$$

Notez que le produit booléen de **A** et **B** est obtenu de manière analogue à l'ordinaire produit de ces matrices, mais avec ajout remplacé par l'opération $\vee$ et par multiplication remplacé par l'opération $\wedge$. Nous donnons un exemple des produits booléens des matrices.

EXEMPLE 8 Trouver le produit booléen de **A** et **B**, où

$$\mathbf{A} = \begin{bmatrix} \text{dix} \\ 0\ 1 \\ \text{dix} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Solution: Le produit booléen $\mathbf{A} \odot \mathbf{B}$ est donné par

$$\mathbf{A} \odot \mathbf{B} = \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

▲

Nous pouvons également définir les puissances booléennes d'une matrice carrée de zéro à un.Ces pouvoirs être utilisé dans nos études ultérieures des chemins dans les graphiques, qui sont utilisés pour modéliser des choses telles que voies de communication dans les réseaux informatiques.

DÉFINITION 10 Soit **A** une matrice carrée de zéro à un et soit r un entier positif. Le r e *pouvoir booléen* de **A** est le produit booléen de r facteurs d' **A** . Le r e produit booléen de **A** est noté $\mathbf{A}^{[r]}$. Par conséquent

$$\text{UNE}^{[r]} = \underbrace{\mathbf{A} \odot \mathbf{A} \odot \mathbf{A} \odot \cdots \odot \mathbf{A}}_{r \text{ fois}}.$$

(Ceci est bien défini car le produit booléen des matrices est associatif.) Nous définissons également $\text{UNE}^{[0]}$ être **je** $_n$.

EXEMPLE 9 Soit $\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$. Trouver $\mathbf{un}^{[n]}$ pour tous les entiers positifs n .

Solution: Nous constatons que

$$\text{UNE}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Nous constatons également que

$$\text{UNE}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad \text{UNE}^{[4]} = \mathbf{A}^{[3]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Un calcul supplémentaire montre que

$$\text{UNE}^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Le lecteur peut maintenant voir que $\mathbf{A}^{[n]} = \mathbf{A}^{[5]}$ pour tous les entiers positifs n avec $n \geq 5$. ▲

Des exercices

1. Soit $\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 2 & 0 & 4 & 6 \\ 1 & 1 & 3 & 7 \end{bmatrix}$.

a) Quelle est la taille de **A** ?
b) Quelle est la troisième colonne de **A** ?
c) Quelle est la deuxième rangée de **A** ?
d) Quel est l'élément de **A** en (3, 2) e position?
e) Qu'est-ce que $\mathbf{A}^t$?

2. Trouvez **A** + **B** , où

a) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ -1 & 2 & 2 \\ 0 & -2 & -3 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -1 & 3 & 5 \\ 2 & 2 & -3 \\ 2 & -3 & 0 \end{bmatrix}$.

b) $\mathbf{A} = \begin{bmatrix} -1 & 0 & 5 & 6 \\ -4 & -3 & 5 & -2 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -3 & 9 & -3 & 4 \\ 0 & -2 & -1 & 2 \end{bmatrix}$.

3. Trouvez **AB** si

a) $\mathbf{A} = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 4 \\ 1 & 3 \end{bmatrix}$.

b) $\mathbf{A} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \\ 2 & 3 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 3 & -2 & -1 \\ 1 & 0 & 2 \end{bmatrix}$.

c) $\mathbf{A} = \begin{bmatrix} 4 & -3 \\ 3 & -1 \\ 0 & -2 \\ -1 & 5 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -1 & 3 & 2 & -2 \\ 0 & -1 & 4 & -3 \end{bmatrix}$.

4. Recherchez le produit **AB** , où

a) $\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ -1 & 1 & 0 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$.

b) $\mathbf{A} = \begin{bmatrix} 1 & -3 & 0 \\ 1 & 2 & 2 \\ 2 & 1 & -1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 1 & -1 & 2 & 3 \\ -1 & 0 & 3 & -1 \\ -3 & -2 & 0 & 2 \end{bmatrix}$.

c) $\mathbf{A} = \begin{bmatrix} 0 & -1 \\ \text{sept} & 2 \\ -4 & -3 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} 4 & -1 & 2 & 3 & 0 \\ -2 & 0 & 3 & 4 & 1 \end{bmatrix}$.

5. Trouvez une matrice **A** telle que

15. Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Trouver une formule pour $\mathbf{A}^n$, chaque fois que n est un entier positif.

16. Montrez que $(\mathbf{A}^t)^t = \mathbf{A}$.

17. Soit **A** et **B** deux matrices $n \times n$. Montre CA

a) $(\mathbf{A} + \mathbf{B})^t = \mathbf{A}^t + \mathbf{B}^t$.
b) $(\mathbf{AB})^t = \mathbf{B}^t\, \text{UNE}^t$

Si **A** et **B** sont $n \times n$ matrices avec **AB** = **BA** = $\mathbf{I}_n$, alors **B**

$$\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \mathbf{A} = \begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}.$$

[*Astuce:* Trouver **A** nécessite que vous résolviez des systèmes de équations.]

6. Trouvez une matrice **A** telle que

$$\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 1 \\ 4 & 0 & 3 \end{bmatrix} \mathbf{A} = \begin{bmatrix} \text{sept} & 1 & 3 \\ 1 & 0 & 3 \\ -1 & -3 & 7 \end{bmatrix}.$$

7. Soit **A** une matrice $m \times n$ et **0** la matrice $m \times n$ qui a toutes les entrées égales à zéro. Montrez que $\mathbf{A} = \mathbf{0} + \mathbf{A} = \mathbf{A} + \mathbf{0}$.

8. Montrer que l'addition matricielle est commutative; C'est, montrent que si **A** et **B** sont tous deux $m \times n$ matrices, alors $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$.

9. Montrez que l'addition de matrice est associative; c'est-à-dire montrer que si **A** , **B** et **C** sont toutes des matrices $m \times n$, alors $\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$.

10. Soit **A** une matrice 3 × 4, **B** une matrice 4 × 5 et **C** une Matrice 4 × 4. Déterminez lequel des produits suivants sont définis et trouvent la taille de ceux qui sont définis.

a) AB **b) BA** **c) AC**

d) CA **e) BC** **f) CB**

11. Que savons-nous des tailles des matrices **A** et **B** si les deux produits **AB** et **BA** sont définis?

12. Dans cet exercice, nous montrons que la multiplication matricielle est tributive sur l'addition de matrice

a) Supposons que **A** et **B** sont des matrices $m \times k$ et que **C** est une matrice $k \times n$. Montrez que $(\mathbf{A} + \mathbf{B})\mathbf{C} = \mathbf{AC} + \mathbf{BC}$.

b) Supposons que **C** est une matrice $m \times k$ et que **A** et **B** sont matrices $k \times n$. Montrez que $\mathbf{C}(\mathbf{A} + \mathbf{B}) = \mathbf{CA} + \mathbf{CB}$.

13. Dans cet exercice, nous montrons que la multiplication matricielle est associatif. Supposons que **A** est une matrice $m \times p$, **B** est une matrice $p \times k$, et **C** est une matrice $k \times n$. Montre CA $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\mathbf{C}$.

14. La matrice $n \times n$ $\mathbf{A} = [a_{ij}]$ est appelée **matrice diagonale** si $a_{ij} = 0$ lorsque $i = j$. Montrer que le produit de deux $n \times n$ les matrices diagonales sont à nouveau une matrice diagonale. Donnez un simple règle générale pour déterminer ce produit.

est appelé l'**inverse** de **A** (cette terminologie est appropriée car une telle matrice **B** est unique) et **A** est dit **inversible** . La notation $\mathbf{B} = \mathbf{A}^{-1}$ indique que **B** est l'inverse de **A** .

18. Montrez que

$$\begin{bmatrix} 2 & 3 & -1 \\ 1 & 2 & 1 \\ -1 & -1 & 3 \end{bmatrix}$$

est l'inverse de

$$\begin{bmatrix} 7 & -8 & 5 \\ -4 & 5 & -3 \\ 1 & -1 & 1 \end{bmatrix}.$$

19. Soit **A** la matrice 2 × 2

$$\mathbf{A} = \begin{bmatrix} un & B \\ C & D \end{bmatrix}.$$

Montrez que si $ad - bc = 0$, alors

$$\text{UNE}^{-1} = \begin{bmatrix} \frac{ré}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{une}{ad - bc} \end{bmatrix}.$$

20. Soit

$$\mathbf{A} = \begin{bmatrix} -1 & 2 \\ 1 & 3 \end{bmatrix}.$$

a) Trouvez $\mathbf{A}^{-1}$. [*Astuce:* utilisez l'exercice 19.]

b) Trouvez $\mathbf{A}^3$.

c) Trouver $(\mathbf{A}^{-1})^3$.

d) Utilisez vos réponses aux points b) et c) pour montrer que $(\mathbf{A}^{-1})^3$ est l'inverse de $\mathbf{A}^3$.

21. Soit **A** une matrice inversible. Montrez que $(\mathbf{A}^n)^{-1} = (\mathbf{A}^{-1})^n$ chaque fois que n est un entier positif.

22. Soit **A** une matrice. Montrer que la matrice $\mathbf{AA}^t$ est symétrique ric. [*Astuce:* Montrez que cette matrice est égale à sa transposition avec l'aide de l'exercice 17b.]

23. Supposons que **A** est une matrice $n \times n$ où n est un positif entier. Montrez que $\mathbf{A} + \mathbf{A}^t$ est symétrique.

Page 206

24. a) Montrer que le système d'équations linéaires simultanées

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &= b_n . \end{aligned}$$

dans les variables $x_1, x_2, \ldots, x_n$ peut être exprimé comme $\mathbf{AX} = \mathbf{B}$, où $\mathbf{A} = [a_{ij}]$, **X** est une matrice $n \times 1$ avec x_i l'entrée dans sa i ème ligne, et **B** est une matrice $n \times 1$ avec b_i l'entrée dans sa i ème ligne.

b) Montrer que si la matrice $\mathbf{A} = [a_{ij}]$ est inversible (comme défini dans le préambule de l'exercice 18), puis le la solution du système dans la partie (a) peut être trouvée en équation $\mathbf{X} = \mathbf{A}^{-1}\mathbf{B}$.

25. Utilisez les exercices 18 et 24 pour résoudre le système

$$\begin{aligned} 7x_1 - 8x_2 + 5x_3 &= 5 \\ -4x_1 + 5x_2 - 3x_3 &= -3 \\ x_1 - x_2 + x_3 &= 0 \end{aligned}$$

26. Soit

$$\begin{bmatrix} 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \end{bmatrix}.$$

28. Trouvez le produit booléen de **A** et **B** , où

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{et} \quad \mathbf{B} = \begin{bmatrix} \text{dix} \\ 0\ 1 \\ 1\ 1 \\ \text{dix} \end{bmatrix}.$$

29. Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Trouver

a) $\mathbf{A}^{[2]}$. **b)** $\mathbf{A}^{[3]}$.

c) $\mathbf{A} \vee \mathbf{A}^{[2]} \vee \mathbf{A}^{[3]}$.

30. Soit **A** une matrice zéro – un. Montre CA

a) $\mathbf{A} \vee \mathbf{A} = \mathbf{A}$. **b)** $\mathbf{A} \wedge \mathbf{A} = \mathbf{A}$.

31. Dans cet exercice, nous montrons que les opérations de rencontre et sont commutatives. Soient **A** et **B** soient $m \times n$ zéro-one matrices. Montre CA

a) $\mathbf{A} \vee \mathbf{B} = \mathbf{B} \vee \mathbf{A}$. **b)** $\mathbf{B} \wedge \mathbf{A} = \mathbf{A} \wedge \mathbf{B}$.

32. Dans cet exercice, nous montrons que les rencontres et les opérations sont associatives. Soient **A** , **B** et **C** soient $m \times n$ zéro-one matrices. Montre CA

a) $(\mathbf{A} \vee \mathbf{B}) \vee \mathbf{C} = \mathbf{A} \vee (\mathbf{B} \vee \mathbf{C})$.

$\mathbf{A} =$ 0 1 et $\mathbf{B} =$ dix

Trouver

a) $\mathbf{A} \vee \mathbf{B}$. **b)** $\mathbf{A} \wedge \mathbf{B}$. **c)** $\mathbf{A} \odot \mathbf{B}$.

27. Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{et} \quad \mathbf{B} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

Trouver

a) $\mathbf{A} \vee \mathbf{B}$. **b)** $\mathbf{A} \wedge \mathbf{B}$. **c)** $\mathbf{A} \odot \mathbf{B}$.

b) $(\mathbf{A} \wedge \mathbf{B}) \wedge \mathbf{C} = \mathbf{A} \wedge (\mathbf{B} \wedge \mathbf{C})$.

33. Nous établirons les lois de distribution de la rencontre sur la rejoindre l'opération dans cet exercice. Soient **A** , **B** et **C** soient $m \times n$ matrices zéro à un. Montre CA

a) $\mathbf{A} \vee (\mathbf{B} \wedge \mathbf{C}) = (\mathbf{A} \vee \mathbf{B}) \wedge (\mathbf{A} \vee \mathbf{C})$.
b) $\mathbf{A} \wedge (\mathbf{B} \vee \mathbf{C}) = (\mathbf{A} \wedge \mathbf{B}) \vee (\mathbf{A} \wedge \mathbf{C})$.

34. Soit **A** soit un $n \times n$ zéro une matrice. Soit **I** le $n \times n$ matrice d'identité. Montrer que $\mathbf{A} \odot \mathbf{I} = \mathbf{I} \odot \mathbf{A} = \mathbf{A}$.

35. Dans cet exercice, nous montrerons que le produit booléen uct de matrices zéro-un est associatif. Supposons que **A** est une matrice $m \times p$ zéro – un, **B** est une matrice $p \times k$ zéro – un matrice, et **C** est une matrice $k \times n$ zéro – un. Montre CA $\mathbf{A} \odot (\mathbf{B} \odot \mathbf{C}) = (\mathbf{A} \odot \mathbf{B}) \odot \mathbf{C}$.

Termes et résultats clés

TERMES

set: une collection d'objets distincts
axiome: une hypothèse de base d'une théorie
paradoxe: une incohérence logique
élément, membre d'un ensemble: un objet dans un ensemble
méthode de fichier: une méthode qui décrit un ensemble en répertoriant ses éléments
set builder notation: la notation qui décrit un ensemble en déclarant une propriété qu'un élément doit avoir pour être membre
∅ (ensemble vide, ensemble nul): l'ensemble sans membres
ensemble universel: l'ensemble contenant tous les objets considérés tion
Diagramme de Venn: une représentation graphique d'un ou de plusieurs ensembles
***S = T* (définir l'égalité):** S et T ont les mêmes éléments
$S \subseteq T$ (*S* est un sous-ensemble de *T*): chaque élément de S est aussi un élément de T
$S \subset T$ (*S* est un sous-ensemble propre de *T*): S est un sous-ensemble de T et $S = T$
ensemble fini: un ensemble avec n éléments, où n est un négatif entier
ensemble infini: un ensemble qui n'est pas fini
$| S |$ (la cardinalité de *S*): le nombre d'éléments dans S
$P(S)$ (l'ensemble de puissance de *S*): l'ensemble de tous les sous-ensembles de S
$A \cup B$ (l'union de *A* et *B*): l'ensemble contenant ces éléments qui sont dans au moins l'un des A et B
$A \cap B$ (l'intersection de *A* et *B*): l'ensemble contenant ceux des éléments qui sont à la fois A et B .

A - B (la différence de *A* et *B*): l'ensemble contenant ceux éléments qui sont en A mais pas en B
A (le complément de *A*): l'ensemble des éléments dans l'universel ensemble qui ne sont pas en A
$A \oplus B$ (la différence symétrique de *A* et *B*): l'ensemble contenant ces éléments dans exactement l'un de A et B
tableau des membres: un tableau montrant la composition des en ensembles
fonction de *A* à *B* : une affectation d'exactement un élément de B à chaque élément de A
domaine de *f* : l'ensemble A , où f est une fonction de A à B
codomaine de *f* : l'ensemble B , où f est une fonction de A à B
***b* est l'image de *a* sous *f* :** $b = f(a)$
***a* est une pré-image de *b* sous *f* :** $f(a) = b$
gamme de *f* : l'ensemble des images de f
sur fonction, surjection: une fonction de A à B telle que chaque élément de B est l'image d'un élément de A
fonction one-to-one, injection: une fonction telle que l'images des éléments de son domaine sont distincts
correspondance biunivoque, bijection: une fonction à la fois un à un et sur
inverse de *f* : la fonction qui inverse la correspondance donné par f (lorsque f est une bijection)
$f \circ g$ (composition de *f* et *g*): la fonction qui attribue $f(g(x))$ à x
$\lfloor x \rfloor$ (fonction plancher): le plus grand entier ne dépassant pas x
$\lceil x \rceil$ (fonction plafond): le plus petit entier supérieur ou égal à x
fonction partielle : une affectation à chaque élément d'un sous-ensemble de le domaine un élément unique dans le codomaine
séquence: une fonction avec domaine qui est un sous-ensemble de l'ensemble de entiers
progression géométrique: une séquence de la forme a , ar , ar^2 , ... , où a et r sont des nombres réels
progression arithmétique: une séquence de la forme a , $a + d$, $a + 2d$, ... , où a et d sont des nombres réels
chaîne: une séquence finie
chaîne vide: une chaîne de longueur zéro
relation de récurrence: une équation qui exprime le n ème terme a_n d'une séquence en termes d'un ou plusieurs des termes précédents de la séquence pour tous les entiers n supérieurs à un particulier entier
$\sum_{i=1}^{n} a_i$: la somme $a_1 + a_2 + \cdots + a_n$
$\prod_{i=1}^{n} a_i$: le produit $a_1 a_2 \cdots a_n$
cardinalité: deux ensembles A et B ont la même cardinalité si il y a une correspondance biunivoque de A à B
ensemble dénombrable: un ensemble fini ou pouvant être placé dans correspondance biunivoque avec l'ensemble d'entiers positifs
ensemble non dénombrable: un ensemble qui n'est pas dénombrable
$\aleph_0$ (aleph null): la cardinalité d'un ensemble dénombrable
c: la cardinalité de l'ensemble des nombres réels
Argument de la diagonalisation de Cantor: une technique de preuve utilisée pour montrer que l'ensemble des nombres réels est indénombrable
fonction calculable: une fonction pour laquelle il existe une programme informatique dans un langage de programmation qui trouve son valeurs
fonction non calculable: une fonction pour laquelle aucun ordinateur programme dans un langage de programmation existe qui trouve son valeurs
hypothèse continuum: la déclaration il n'y pas d' ensemble A existe tel que $\aleph_0 < | A | < \mathbf{c}$
matrice: un tableau rectangulaire de nombres
ajout de matrice: voir page 178
multiplication matricielle: voir page 179
$\mathbf{I}_n$ (matrice d'identité d'ordre *n*): la matrice $n \times n$ qui a entrées égales à 1 sur sa diagonale et 0 ailleurs
UNE (transposition de A): la matrice obtenue à partir de **A** par échange des lignes et des colonnes
matrice symétrique: une matrice est symétrique si elle est égale à sa transpose
matrice zéro-un: matrice dont chaque entrée est égale à 0 ou 1
$\mathbf{A} \vee \mathbf{B}$ (la jonction de A et B): voir page 181
$\mathbf{A} \wedge \mathbf{B}$ (la rencontre de A et B): voir page 181
$\mathbf{A} \odot \mathbf{B}$ (le produit booléen de A et B): voir page 182

RÉSULTATS

Les identités d'ensemble données dans le tableau 1 de la section 2.2
Les formules de sommation du tableau 2 de la section 2.4
L'ensemble des nombres rationnels est dénombrable.
L'ensemble des nombres réels est indénombrable.

Questions de révision

1. Expliquez ce que signifie qu'un ensemble est un sous-ensemble d'un autre ensemble. Comment prouver qu'un ensemble est un sous-ensemble d'un autre ensemble?

2. Qu'est-ce que l'ensemble vide? Montrer que l'ensemble vide est un sous-ensemble de chaque ensemble.

3. a) Définir $|S|$, la cardinalité de l'ensemble S.
b) Donnez une formule pour $|A \cup B|$, où A et B sont des ensembles.

4. a) Définir l'ensemble de la puissance d'un ensemble S.
b) Quand l'ensemble vide est-il dans l'ensemble de puissance d'un ensemble S ?
c) Combien d'éléments l'ensemble de puissance d'un ensemble S avec n éléments ont?

5. a) Définissez l'union, l'intersection, la différence et la symétrique métrique de deux ensembles.
b) Quels sont l'union, l'intersection, la différence et la symétrique métrique de l'ensemble des entiers positifs et la ensemble d'entiers impairs?

6. a) Explique ce que signifie que deux ensembles sont égaux.
b) Décrivez autant de façons que possible de montrer que deux ensembles sont égaux.
c) Montrer d'au moins deux manières différentes que les ensembles $A - (B \cap C)$ et $(A - B) \cup (A - C)$ sont égaux.

7. Expliquer la relation entre les équivalences logiques et définir des identités.

8. a) Définissez le domaine, le domaine de codage et la plage d'une fonction.
b) Soit $f(n)$ la fonction de l'ensemble des nombres entiers au ensemble d'entiers tels que $f(n) = n^2 + 1$. Quels sont les domaine, codomaine et plage de cette fonction?

9. a) Définissez ce que cela signifie pour une fonction à partir de entiers positifs à l'ensemble des entiers positifs à Un par un.
b) Définissez ce que cela signifie pour une fonction à partir de l'ensemble des entiers positifs à l'ensemble des entiers positifs à sur.
c) Donnez un exemple de fonction de l'ensemble des posi- entiers positifs à l'ensemble des entiers positifs qui est à la fois un à un et sur.
d) Donner un exemple d'une fonction de l'ensemble des positifs des entiers à l'ensemble d'entiers positifs qui est un à un mais pas sur.
e) Donnez un exemple de fonction de l'ensemble de posi- entiers positifs à l'ensemble des entiers positifs qui ne sont pas un à un, mais est sur.
f) Donner un exemple d'une fonction de l'ensemble des positifs entiers à l'ensemble d'entiers positifs qui n'est ni un à un ni sur.

10. a) Définissez l'inverse d'une fonction.
b) Quand une fonction a-t-elle un inverse?
c) La fonction $f(n) = 10 - n$ de l'ensemble des gers à l'ensemble des entiers ont un inverse? Si oui, quoi est-ce?

11. a) Définissez les fonctions de plancher et de plafond à partir de nombres réels à l'ensemble des entiers.
b) Pour quels nombres réels x est-il vrai que $\lfloor x \rfloor = \lceil x \rceil$?

12. Conjecturer une formule pour les termes de la séquence qui commence 8 , 14 , 32 , 86 , 248 et trouver les trois termes suivants de votre séquence.

13. Supposons que *une* $_n = a_{n-1} - 5$ en ce $n = 1, 2, \ldots$. Trouvez un mula pour *un* $_n$.

14. Quelle est la somme des termes de la progression géométrique $a + ar + \cdots + ar^n$ quand $r = 1$?

15. Montrer que l'ensemble des entiers impairs est dénombrable.

16. Donnez un exemple d'un ensemble indénombrable.

17. Définir le produit de deux matrices **A** et **B** . Quand cest produit défini?

18. Montrer que la multiplication matricielle n'est pas commutative.

Exercices supplémentaires

1. Soit A l'ensemble des mots anglais contenant la lettre x , et que B soit l'ensemble des mots anglais qui contiennent le lettre q . Exprimez chacun de ces ensembles comme une combinaison de A et B .
a) L'ensemble des mots anglais qui ne contiennent pas la lettre x .
b) L'ensemble des mots anglais qui contiennent à la fois un x et un q .
c) L'ensemble des mots anglais qui contiennent un x mais pas un q .
d) L'ensemble des mots anglais qui ne contiennent ni un x ou a q .
e) L'ensemble des mots anglais qui contiennent un x ou un q , mais pas les deux.

2. Montrez que si A est un sous-ensemble de B , alors l'ensemble de puissance de A est un sous - ensemble de l'ensemble de puissance B .

3. Supposons que A et B sont des ensembles tels que l'ensemble de puissance de A est un sous - ensemble de l'ensemble de puissance B . S'ensuit-il que A est un sous-ensemble de B ?

4. Soit **E** l'ensemble des entiers pairs et **O** le nombre ensemble d'entiers impairs. Comme d'habitude, laissez **Z** désigner l'ensemble de tous entiers. Déterminez chacun de ces ensembles.

a) $\mathbf{E} \cup \mathbf{O}$ **b)** $\mathbf{E} \cap \mathbf{O}$ **c)** $\mathbf{Z} - \mathbf{E}$ **d)** $\mathbf{Z} - \mathbf{O}$

5. Montrez que si A et B sont des ensembles, alors $A - (A - B) = A \cap B$.

6. Soit A et B *des* ensembles. Montrer que $A \subseteq B$ si et seulement si $A \cap B = A$.

7. Soit A, B et C *des* ensembles. Montrez que $(A - B) - C$ n'est pas nécessairement égal à $A - (B - C)$.

8. Supposons que A, B et C sont des ensembles. Prouvez ou réfutez cela $(A - B) - C = (A - C) - B$.

9. Supposons que A, B, C et D sont des ensembles. Prouver ou réfuter que $(A - B) - (C - D) = (A - C) - (B - D)$.

10. Montrez que si A et B sont des ensembles finis, alors $|A \cap B| \leq |A \cup B|$. Déterminez quand cette relation est une égalité.

11. Soit A et B soient ensembles dans un ensemble universel fini U . Liste des suivant par ordre croissant de taille.
a) $|A|$, $|A \cup B|$, $|A \cap B|$, $|U|$, $|\varnothing|$
b) $|A - B|$, $|A \oplus B|$, $|A| + |B|$, $|A \cup B|$, $|\varnothing|$

12. Soit A et B des sous - ensembles de l'ensemble universel fini U . Spectacle que $|A \cap B| = |U| - |A| - |B| + |A \cap B|$.

13. Soit f et g *des* fonctions de {1 , 2 , 3 , 4} à { a, b, c, d } et de { a, b, c, d } à {1 , 2 , 3 , 4}, respectivement, avec $f(1) = d$, $f(2) = c$, $f(3) = a$, et $f(4) = b$, et $g(a) = 2$, $g(b) = 1$, $g(c) = 3$ et $g(d) = 2$.
a) F est -il un à un? Est - g one-to-one?
b) Est-ce que f est sur? Est-ce que g est ?
c) Est-ce que f ou g ont un inverse? Si oui, trouvez ceci inverse.

14. Supposons que f soit une fonction de A à B où A et B sont des ensembles finis. Expliquez pourquoi $|f(S)| \leq |S|$ pour tous les sous-ensembles S de A .

15. Supposons que f soit une fonction de A à B où A et B sont des ensembles finis. Expliquez pourquoi $|f(S)| = |S|$ pour tous les sous-ensembles S de A si et seulement si f est un à un.

On suppose que f est une fonction de A à B . Nous définissons la fonction tion S_f de $P(A)$ à $P(B)$ par la règle $S_f(X) = f(X)$ pour chaque sous - ensemble X de A . De même, nous définissons la fonction $S_{f^{-1}}$ de $P(B)$ à $P(A)$ par la règle $S_{f^{-1}}(Y) = f^{-1}(Y)$ pour chacun sous - ensemble Y de B . Ici, nous utilisons la définition 4 et la définition nition de l'image inverse d'un ensemble trouvé dans le préambule de Exercice 42, tous deux dans la section 2.3.

∗ **16.** On suppose que f est une fonction de l'ensemble A à l'ensemble B .

Prouve-le

a) si f est un à un, alors S_f est une fonction un à un de $P(A)$ à $P(B)$.

b) si f est sur la fonction, alors S_f est une fonction sur de $P(A)$ à $P(B)$.

c) si f est sur la fonction, alors $S_{f^{-1}}$ est une fonction biunivoque de $P(B)$ à $P(A)$.

d) si f est un à un, alors $S_{f^{-1}}$ est une fonction sur de $P(B)$ à $P(A)$.

e) si f est une correspondance biunivoque, alors S_f est une correspondance un correspondance *individuelle* de $P(A)$ à $P(B)$ et $S_{f^{-1}}$ est une correspondance biunivoque de $P(B)$ à $P(A)$. [*Astuce:* utilisez les parties (a) - (d).]

17. Montrer que si f et g sont des fonctions de A à B et $S_f = S_g$ (en utilisant la définition du préambule de l'exercice 16), alors $f(x) = g(x)$ pour tout $x \in A$.

18. Montrer que si n est un entier, alors $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$.

19. Pour quels nombres réels x et y est-il vrai que $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$?

20. Pour quels nombres réels x et y est-il vrai que $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$?

21. Pour quels nombres réels x et y est-il vrai que $\lceil x + y \rceil = \lceil x \rceil + \lfloor y \rfloor$?

22. Montrer que $\lfloor n/2 \rfloor \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$ pour tous les entiers n .

23. Démontrer que si m est un entier, alors $\lfloor x \rfloor + \lfloor m - x \rfloor = m - 1$, sauf si x est un entier, auquel cas il est égal à m .

24. Démontrez que si x est un nombre réel, alors $\lfloor \lfloor x/2 \rfloor /2 \rfloor = \lfloor x/4 \rfloor$.

25. Démontrer que si n est un nombre entier impair, alors $\lceil n^2/4 \rceil = (n^2 + 3)/4$.

26. Démontrer que si m et n sont des entiers positifs et que x est un réel nombre, puis

$$\left\lfloor \frac{\lfloor x \rfloor + n}{m} \right\rfloor = \left\lfloor \frac{x + n}{m} \right\rfloor .$$

∗ **27.** Démontrer que si m est un entier positif et x est un nombre réel, ensuite

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \left\lfloor x + \frac{2}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor .$$

∗ **28.** Nous définissons les **nombres Ulam** en mettant $u_1 = 1$ et $u_2 = 2$. De plus, après avoir déterminé si l'in- tegers inférieurs à n sont des nombres Ulam, nous fixons n égal à le prochain nombre Ulam s'il peut être écrit uniquement comme somme de deux nombres Ulam différents. Notez que $u_3 = 3$, $u_4 = 4$, $u_5 = 6$ et $u_6 = 8$.

a) Trouvez les 20 premiers nombres d'Ulam.

b) Démontrer qu'il existe une infinité de nombres Ulam.

29. Déterminez la valeur de $\prod_{k=1}^{100} \frac{k+1}{k}$. (La notation utilisée ici pour les produits est défini dans le préambule de l'exercice 43 dans la section 2.4.)

∗ **30.** Déterminer une règle pour générer les termes de la séquence qui commence $1, 3, 4, 8, 15, 27, 50, 92, \ldots$, et trouver le suivant quatre termes de la séquence.

∗ **31.** Déterminer une règle pour générer les termes de la séquence qui commence $2, 3, 3, 5, 10, 13, 39, 43, 172, 177, 885, 891, \ldots$, et trouvez les quatre termes suivants de la séquence.

32. Montrer que l'ensemble des nombres irrationnels est un nombre indénombrable ensemble.

33. Montrer que l'ensemble S est un ensemble dénombrable s'il existe une fonction tion f de S aux entiers positifs tels que $f^{-1}(j)$ est dénombrable chaque fois que j est un entier positif.

34. Montrer que l'ensemble de tous les sous-ensembles finis de l'ensemble des positifs entiers est un ensemble dénombrable.

∗∗ **35.** Montrez que $|\mathbf{R} \times \mathbf{R}| = |\mathbf{R}|$. [*Astuce:* utilisez le Schröder- Théorème de Bernstein pour montrer que $|(0, 1) \times (0, 1)| = |(0, 1)|$. Pour construire une injection de $(0, 1) \times (0, 1)$ à $(0, 1)$, supposons que $(x, y) \in (0, 1) \times (0, 1)$. Carte (x, y) au nombre avec une expansion décimale formé par l'altération entre les chiffres dans les extensions décimales de x et y , qui ne se terminent pas par une chaîne infinie de 9.]

∗∗ **36.** Montrer que **C** , l'ensemble des nombres complexes a le même cardinalité comme **R** , l'ensemble des nombres réels.

37. Trouver $\mathbf{A}^n$ si **A** est

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} .$$

38. Montrer que si $\mathbf{A} = c\,\mathbf{I}$, où c est un nombre réel et **I** est le $n \times n$ matrice d'identité, alors $\mathbf{AB} = \mathbf{BA}$ chaque fois que **B** est un matrice $n \times n$.

39. Montrer que si **A** est une matrice 2×2 telle que $\mathbf{AB} = \mathbf{BA}$ quand- jamais **B** est une matrice 2×2, alors $\mathbf{A} = c\,\mathbf{I}$, où c est un réel nombre et **I** est la matrice d'identité 2×2.

40. Montrer que si **A** et **B** sont des matrices inversibles et **AB** existe, alors $(\mathbf{AB})^{-1} = \mathbf{B}^{-1}$ **UNE**$^{-1}$.

41. Soit **A** une matrice $n \times n$ et soit **0** la matrice $n \times n$ dont toutes les entrées sont nulles. Montrez que les éléments suivants sont vrai.

a) $\mathbf{A} \odot \mathbf{0} = \mathbf{0} \odot \mathbf{A} = \mathbf{0}$

b) $\mathbf{A} \vee \mathbf{0} = \mathbf{0} \vee \mathbf{A} = \mathbf{A}$

c) $\mathbf{A} \wedge \mathbf{0} = \mathbf{0} \wedge \mathbf{A} = \mathbf{0}$

Projets informatiques

Écrivez des programmes avec l'entrée et la sortie spécifiées.

1. Étant donné les sous-ensembles A et B d'un ensemble de n éléments, utilisez bit chaînes pour trouver A , $A \cup B$, $A \cap B$, $A - B$ et $A \oplus B$.

2. Étant donné les multisets A et B du même ensemble universel, trouvez $A \cup B$, $A \cap B$, $A - B$ et $A + B$ (voir préambule de l'Exercise 61 de la section 2.2).

3. Étant donné les ensembles flous A et B , trouvez A , $A \cup B$ et $A \cap B$ (voir préambule de l'exercice 63 de la section 2.2).

4. Étant donné une fonction f de $\{1 , 2 , ..., n \}$ à l'ensemble des entiers, déterminer si f est un à un.

5. Étant donné une fonction f de $\{1 , 2 , ..., n \}$ à elle-même, déterminez si f est sur.

6. Étant donné une bijection f de l'ensemble $\{1 , 2 , ..., n \}$ à lui-même, trouver f^{-1} .

7. Étant donné une matrice $m \times k$ **A** et une matrice $k \times n$ **B** , trouvez **AB** .

8. Étant donné une matrice carrée **A** et un entier positif n , trouvez $\mathbf{A}^n$.

9. Étant donné une matrice carrée, déterminez si elle est symétrique.

10. Étant donné deux matrices booléennes $m \times n$, trouvez leur rencontre et joindre.

11. Étant donné une matrice booléenne $m \times k$ **A** et une booléenne $k \times n$ matrice **B** , trouver le produit booléen de **A** et **B** .

12. Étant donné une matrice booléenne carrée **A** et un entier positif n , trouver $\mathbf{un}^{[n]}$.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Étant donné deux ensembles finis, énumérer tous les éléments du produit cartésien uct de ces deux ensembles.

2. Étant donné un ensemble fini, listez tous les éléments de son ensemble de puissance.

3. Calculez le nombre de fonctions biunivoque à partir d'un ensemble S à un ensemble T , où S et T sont des ensembles finis de différentes tailles. Pouvez vous déterminez une formule pour le nombre de ces fonctions? (Nous trouverons une telle formule au chapitre 6.)

4. Calculez le nombre de fonctions sur d'un ensemble S à un ensemble T , où S et T sont des ensembles finis de différentes tailles. Pouvez vous déterminez une formule pour le nombre de ces fonctions? (Nous trouverons une telle formule au chapitre 8.)

∗ **5.** Développer un ensemble de règles différentes pour générer le termes d'une séquence et d'un programme de sélection aléatoire l'une de ces règles et la séquence particulière générée en utilisant ces règles. Faites cette partie d'un programme interactif qui invite au prochain terme de la séquence et à déterminer mine si la réponse est le prochain terme prévu.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Discutez de la façon dont une théorie axiomatique des ensembles peut être éviter le paradoxe de Russell. (Voir l'exercice 46 de la section 2.1.)

2. Recherche où le concept de fonction est apparu pour la première fois, et décrire comment ce concept a été utilisé pour la première fois.

3. Expliquez les différentes manières dont l' *Encyclopédie de Les séquences entières* se sont avérées utiles. Décrivez également quelques-unes des séquences les plus inhabituelles de cette encyclopédie et comment ils surviennent.

4. Définissez la séquence ECG récemment inventée et décrivez certaines de ses propriétés et des questions ouvertes à ce sujet.

5. Recherchez la définition d'un nombre transcendantal. Explique comment montrer que de tels nombres existent et comment bers peuvent être construits. Quels numéros célèbres peuvent être montré pour être transcendantal et pour lequel les numéros célèbres est-il encore inconnu s'ils sont transcendantaux?

6. Développer la discussion de l'hypothèse du continuum dans le texte.

CHAPITRE

Des algorithmes

De nombreux problèmes peuvent être résolus en les considérant comme des cas particuliers de problèmes généraux. Par exemple, considérons le problème de la localisation du plus grand entier dans la séquence 101, 12, 144, 212, 98. Ceci est un cas spécifique du problème de localisation du plus grand entier dans une séquence d'entiers. Pour résoudre ce problème général, nous devons donner un algorithme, qui spécifie une séquence des étapes utilisées pour résoudre ce problème général. Nous étudierons des algorithmes pour résoudre de nombreux types de problèmes dans ce livre. Par exemple, dans ce chapitre, nous présenterons des algorithmes pour deux des problèmes les plus importants en informatique, la recherche d'un élément dans une liste et trier une liste afin que ses éléments soient dans un certain ordre prescrit, comme augmenter, diminuer ou alphabétique. Plus tard dans le livre, nous développerons des algorithmes qui trouveront le plus grand diviseur commun de deux entiers, qui génèrent tous les ordres d'un ensemble fini, qui trouvent le chemin le plus court entre nœuds dans un réseau, et pour résoudre de nombreux autres problèmes.

Nous introduirons également la notion de paradigme algorithmique, qui fournit une méthode de conception d'algorithmes. En particulier, nous discuterons des algorithmes de force brute, qui trouver des solutions en utilisant une approche simple sans introduire d'intelligence. Nous allons également discuter d'algorithmes gourmands, une classe d'algorithmes utilisés pour résoudre les problèmes d'optimisation. Les preuves sont important dans l'étude des algorithmes. Dans ce chapitre, nous illustrons cela en prouvant qu'un l'algorithme gourmand trouve toujours une solution optimale.

Une considération importante concernant un algorithme est sa complexité de calcul, qui mesure le temps de traitement et la mémoire de l'ordinateur requis par l'algorithme pour résoudre problèmes d'une taille particulière. Pour mesurer la complexité des algorithmes, nous utilisons big- *0* et big-Notation thêta, que nous développons dans ce chapitre. Nous illustrerons l'analyse de la complexité des algorithmes dans ce chapitre, en se concentrant sur le temps qu'un algorithme prend pour résoudre un problème. Fourrure-En plus, nous allons discuter de ce que signifie la complexité temporelle d'un algorithme en pratique et termes théoriques.

Algorithmes

introduction

Il existe de nombreuses classes générales de problèmes qui se posent en mathématiques discrètes. Par exemple: étant donné une séquence d'entiers, trouvez le plus grand; étant donné un ensemble, listez tous ses sous-ensembles; étant donné un ensemble des entiers, les mettre dans l'ordre croissant; étant donné un réseau, trouver le chemin le plus court entre deux sommets. Face à un tel problème, la première chose à faire est de construire un modèle qui traduit le problème dans un contexte mathématique. Structures discrètes utilisées dans de tels modèles inclure des ensembles, des séquences et des fonctions - structures discutées dans le chapitre 2 - ainsi que d'autres structures comme permutations, relations, graphes, arbres, réseaux et machines à états finis - concepts qui seront discutés dans les chapitres suivants.

La mise en place du modèle mathématique approprié n'est qu'une partie de la solution. Pour compléter le solution, une méthode est nécessaire pour résoudre le problème général à l'aide du modèle. Idéalement, quoi est nécessaire est une procédure qui suit une séquence d'étapes qui mène à la réponse souhaitée. Tel une séquence d'étapes est appelée un **algorithme** .

DÉFINITION 1 Un *algorithme* est une séquence finie d'instructions précises pour effectuer un calcul ou pour résoudre un problème.

Le terme *algorithme* est une corruption du nom *al-Khowarizmi* , mathématicien du neuvième siècle, dont le livre sur les chiffres hindous est la base de la notation décimale moderne.Initialement, le mot *algorism a* été utilisé pour les règles d'exécution de l'arithmétique en utilisant la notation décimale. *L'algorisme est* devenu l' *algorithme des* mots au XVIIIe siècle. Avec un intérêt croissant dans les machines informatiques, le concept d'algorithme a pris un sens plus général, inclure toutes les procédures définies pour résoudre les problèmes, pas seulement les procédures pour effectuer arithmétique. (Nous discuterons des algorithmes pour effectuer l'arithmétique avec des entiers dans le chapitre 4.)

Dans ce livre, nous discuterons des algorithmes qui résolvent une grande variété de problèmes.Dans ce section, nous allons utiliser le problème de trouver le plus grand entier dans une séquence finie d'entiers pour illustrer le concept d'un algorithme et les propriétés des algorithmes.Nous décrirons également algorithmes pour localiser un élément particulier dans un ensemble fini.Dans les sections suivantes, les procédures pour trouver le plus grand diviseur commun de deux nombres entiers, pour trouver le chemin le plus court entre deux points dans un réseau, pour multiplier les matrices, etc., seront discutés.

EXEMPLE 1 Décrire un algorithme pour trouver la valeur maximale (la plus grande) dans une séquence finie d'entiers.

Même si le problème de trouver l'élément maximum dans une séquence est relativement trivial, il fournit une bonne illustration du concept d'un algorithme.En outre, il existe de nombreux cas où le plus grand entier dans une séquence finie d'entiers est requis.Par exemple, une université Il faudra peut-être trouver le meilleur score à un examen concurrentiel passé par des milliers d'étudiants.Ou une organisation sportive peut vouloir identifier le membre avec la note la plus élevée chaque mois. Nous voulons développer un algorithme qui peut être utilisé chaque fois que le problème de trouver le plus grand apparaît dans une séquence finie d'entiers.

Nous pouvons spécifier une procédure pour résoudre ce problème de plusieurs manières.Une méthode consiste simplement à utilisez la langue anglaise pour décrire la séquence des étapes utilisées.Nous proposons désormais une telle solution.

Solution de l'exemple 1: Nous effectuons les étapes suivantes.

1. Définissez le maximum temporaire égal au premier entier de la séquence.(Le temporaire maximum sera le plus grand entier examiné à n'importe quelle étape de la procédure.)
2. Comparez le prochain entier de la séquence au maximum temporaire, et s'il est plus grand que le maximum temporaire, définissez le maximum temporaire égal à cet entier.
3. Répétez l'étape précédente s'il y a plus d'entiers dans la séquence.
4. Arrêtez lorsqu'il n'y a plus d'entiers dans la séquence.Le maximum temporaire à ce le point est le plus grand entier de la séquence.

▲

Un algorithme peut également être décrit à l'aide d'un langage informatique.Cependant, lorsque cela est fait, seules les instructions autorisées dans la langue peuvent être utilisées.Cela conduit souvent à une description de l'algorithme qui est compliqué et difficile à comprendre.En outre, parce que de nombreux les langages de programmation sont couramment utilisés, il ne serait pas souhaitable de choisir un Langue. Ainsi, au lieu d'utiliser un langage informatique particulier pour spécifier des algorithmes, un formulaire du **pseudocode** , décrit dans l'annexe 3, sera utilisé dans ce livre. (Nous décrirons également algorithmes utilisant la langue anglaise.) Le pseudocode fournit une étape intermédiaire entre

ABU JA'FAR MOHAMMED IBN MUSA AL-KHOWARIZMI (C. 780 – C. 850) al-Khowarizmi, un astronomère et mathématicien, était membre de la Maison de la Sagesse, une académie de scientifiques à Bagdad. Le nom al-Khowarizmi signifie «de la ville de Kowarzizm», qui faisait alors partie de la Perse, mais qui est maintenant appelé *Khiva* et fait partie de l'Ouzbékistan. al-Khowarizmi a écrit des livres sur les mathématiques, l'astronomie et la géographie. Les Européens de l'Ouest ont découvert l'algèbre pour la première fois grâce à ses œuvres. Le mot *algèbre* vient d'al-jabr, une partie de le titre de son livre *Kitab al-jabr w'al muquabala* . Ce livre a été traduit en latin et a été largement utilisé cahier de texte. Son livre sur l'utilisation des chiffres hindous décrit les procédures des opérations arithmétiques utilisant ces chiffres. Les auteurs européens ont utilisé une corruption latine de son nom, qui a évolué plus tard vers le mot *algorithme,* pour décrire le sujet de l'arithmétique avec des chiffres hindous.

une description en langue anglaise d'un algorithme et une implémentation de cet algorithme dans un langage de programmation.Les étapes de l'algorithme sont spécifiées à l'aide d'instructions ressemblant à ceux utilisés dans les langages de programmation.Cependant, en pseudocode, les instructions utilisées peuvent inclure toute opération ou instruction bien définie.Un programme informatique peut être produit en tout langage informatique utilisant la description du pseudocode comme point de départ.

Le pseudocode utilisé dans ce livre est conçu pour être facilement compris.Il peut servir de étape intermédiaire dans la construction de programmes mettant en œuvre des algorithmes dans l’une des différents langages de programmation.Bien que ce pseudocode ne suive pas la syntaxe de Java, C, C ++, ou tout autre langage de programmation, étudiants familiers avec une programmation moderne la langue le trouvera facile à suivre.Une différence clé entre ce pseudocode et le code dans un langage de programmation est que nous pouvons utiliser n'importe quelle instruction bien définie même si cela prendrait plusieurs lignes de code pour implémenter cette instruction. Les détails du pseudocode utilisé dans le texte sont données à l'annexe 3. Le lecteur doit se référer à cette annexe chaque fois que le besoin s'en fait sentir.

Une description pseudocode de l'algorithme pour trouver l'élément maximum dans un fini la séquence suit.

ALGORITHME 1 **Recherche de l'élément maximum dans une séquence finie.**

procédure *max* $(a_1, a_2, \ldots, a_n$: entiers)
max : $= a_1$
pour $i := 2$ **à** n
  si *max* $< a_i$ **alors** *max* $:= a_i$
return *max* { *max* est le plus grand élément}

Cet algorithme attribue d'abord le terme initial de la séquence, a_1, à la variable *max.* Le «pour» La boucle est utilisée pour examiner successivement les termes de la séquence. Si un terme est supérieur à l'actuel valeur *max,* elle est affectée à la nouvelle valeur *max.*

PROPRIÉTÉS DES ALGORITHMES Il existe plusieurs propriétés que les algorithmes généralement partager. Ils sont utiles à garder à l'esprit lorsque les algorithmes sont décrits. Ces propriétés sont:

- *Entrée.* Un algorithme a des valeurs d'entrée à partir d'un ensemble spécifié.
- *Sortie.* À partir de chaque ensemble de valeurs d'entrée, un algorithme produit des valeurs de sortie à partir ensemble ified. Les valeurs de sortie sont la solution au problème.
- *Définition.* Les étapes d'un algorithme doivent être définies avec précision.
- *Exactitude.* Un algorithme doit produire les valeurs de sortie correctes pour chaque ensemble d'entrées valeurs.
- *Finitude.* Un algorithme devrait produire la sortie souhaitée après un fini (mais peut-être grand) nombre d'étapes pour n'importe quelle entrée dans l'ensemble.
- *Efficacité.* Il doit être possible d'effectuer chaque étape d'un algorithme exactement et dans un durée limitée.
- *Généralité.* La procédure doit être applicable à tous les problèmes de la forme souhaitée, et non juste pour un ensemble particulier de valeurs d'entrée.

EXEMPLE 2 Montrer que l'algorithme 1 pour trouver l'élément maximum dans une séquence finie d'entiers a tous les propriétés répertoriées.

Solution: l'entrée de l'algorithme 1 est une séquence d'entiers. La sortie est le plus grand entier dans la séquence. Chaque étape de l'algorithme est définie avec précision, car seules les affectations, un boucle finie et des instructions conditionnelles se produisent. Pour montrer que l'algorithme est correct, il faut montrent que lorsque l'algorithme se termine, la valeur de la variable *max* est égale au maximum

des termes de la séquence. Pour voir cela, notez que la valeur initiale de *max* est le premier terme de la séquence; à mesure que les termes successifs de la séquence sont examinés, *max* est mis à jour à la valeur d'un terme si le terme dépasse le maximum des termes précédemment examinés. Ce (informel) L'argument montre que lorsque tous les termes ont été examinés, *max* est égal à la valeur du plus grand terme. (Une preuve rigoureuse de cela nécessite des techniques développées dans la section 5.1.) L'algorithme utilise un nombre fini d'étapes, car il se termine après que tous les entiers de la séquence ont été examinés. L'algorithme peut être exécuté en un temps limité car chaque étape est soit une comparaison ou une affectation, il y a un nombre fini de ces étapes, et chacune de ces étapes deux opérations prennent un temps limité. Enfin, l'algorithme 1 est général, car il peut être utilisé pour trouver le maximum de toute séquence finie d'entiers. ▲

Recherche d'algorithmes

Le problème de la localisation d'un élément dans une liste ordonnée se produit dans de nombreux contextes. Par exemple, un programme qui vérifie l'orthographe des mots les recherche dans un dictionnaire, qui n'est qu'un liste ordonnée de mots. Les problèmes de ce type sont appelés **problèmes de recherche** . Nous discuterons plusieurs algorithmes de recherche dans cette section. Nous étudierons le nombre d'étapes utilisées par chacun de ces algorithmes dans la section 3.3.

Le problème de recherche général peut être décrit comme suit: Localisez un élément x dans une liste de des éléments distincts $a_1, a_2, \ldots, a_n$, ou déterminer qu'il ne figure pas dans la liste. La solution à cette recherche le problème est l'emplacement du terme dans la liste qui est égal à x (c'est-à-dire, i est la solution si $x = a_i$) et vaut 0 si x n'est pas dans la liste.

LA RECHERCHE LINÉAIRE Le premier algorithme que nous allons présenter est appelé la **recherche linéaire** , ou **recherche séquentielle** , algorithme. L'algorithme de recherche linéaire commence par comparer x et a_1 . Lorsque $x = a_1$, la solution est l'emplacement d'un_1 , à savoir 1. Lorsque $x = a_1$, comparer x avec un_2 . Si $x = a_2$, la solution est l'emplacement d'un_2 , à savoir, 2. Lorsque $x = a_2$, comparer x avec un_3 . Continuer ce processus, en comparant x successivement à chaque terme de la liste jusqu'à ce qu'une correspondance soit trouvée, où la solution est l'emplacement de ce terme, sauf si aucune correspondance ne se produit. Si la liste entière a été recherché sans localiser x , la solution est 0. Le pseudocode de l'algorithme de recherche linéaire s'affiche en tant qu'algorithme 2.

ALGORITHME 2 L'algorithme de recherche linéaire.

recherche linéaire de **procédure** (x : entier, a_1 , a_2 , ..., a_n : entiers distincts)
i : = 1
tandis que ($i \leq n$ et $x = a_i$)
  i : = i + 1
si $i \leq n$ **alors** *emplacement* : = i
sinon *emplacement* : = 0
return *location* { *location* est l'indice du terme égal à x , ou égal à 0 si x n'est pas trouvé}

LA RECHERCHE BINAIRE Nous allons maintenant considérer un autre algorithme de recherche. Cet algorithme peut être utilisé lorsque la liste a des termes apparaissant par ordre de taille croissante (par exemple: si le les termes sont des nombres, ils sont énumérés du plus petit au plus grand;si ce sont des mots, ils sont listés par ordre lexicographique ou alphabétique). Ce deuxième algorithme de recherche est appelé le **binaire algorithme de recherche** . Il procède en comparant l'élément à localiser au moyen terme de la liste. La liste est ensuite divisée en deux sous-listes plus petites de la même taille, ou lorsque l'une de ces les listes plus petites ont un terme de moins que l'autre. La recherche se poursuit en restreignant la recherche à la sous-liste appropriée sur la base de la comparaison de l'élément à localiser et du milieu terme. Dans la section 3.3, il sera montré que l'algorithme de recherche binaire est beaucoup plus efficace que l'algorithme de recherche linéaire. L'exemple 3 montre comment fonctionne une recherche binaire.

EXEMPLE 3 Pour rechercher 19 dans la liste

1 2 3 5 6 7 8 10 12 13 15 16 18 19 20 22 ,

diviser d'abord cette liste, qui comprend 16 termes, en deux listes plus petites de huit termes chacune, à savoir,

1 2 3 5 6 7 8 10   12 13 15 16 18 19 20 22.

Ensuite, comparez 19 et le terme le plus grand de la première liste. Parce que 10 < 19, la recherche de 19 peut être limité à la liste contenant les 9e à 16e termes de la liste originale. Ensuite, divisez cette liste, qui a huit termes, dans les deux listes plus petites de quatre termes chacune, à savoir,

12 13 15 16   18 19 20 22 .

Parce que 16 < 19 (comparant 19 au terme le plus grand de la première liste), la recherche est limitée à la deuxième de ces listes, qui contient les 13e à 16e termes de la liste originale. le la liste 18 19 20 22 est divisée en deux listes, à savoir:

18 19   20 22 .

Parce que 19 n'est pas supérieur au terme le plus long de la première de ces deux listes, qui est aussi 19, le la recherche est limitée à la première liste: 18 19, qui contient les 13e et 14e termes de l'original liste. Ensuite, cette liste de deux termes est divisée en deux listes d'un terme chacune: 18 et 19. Parce que 18 < 19, la recherche se limite à la deuxième liste: la liste contenant le 14e terme de la liste, qui est 19. Maintenant que la recherche a été réduite à un terme, une comparaison est faite, et 19 correspond au 14e terme de la liste d'origine. ▲

Nous spécifions maintenant les étapes de l'algorithme de recherche binaire. Pour rechercher l'entier x dans le indiquez a_1 , a_2 , ..., a_n , où $a_1 < a_2 < \cdots < a_n$, commencez par comparer x au terme moyen a_m de la liste, où $m = \lfloor (n + 1) / 2 \rfloor$. (Rappelez-vous que $\lfloor x \rfloor$ est le plus grand entier ne dépassant pas x .) Si $x > a_m$, la recherche de x est limitée à la seconde moitié de la liste, qui est a_{m+1} , a_{m+2} , ..., a_n . Si x n'est pas supérieur à a_m , la recherche de x est limitée à la première moitié de la liste, qui est a_1 , a_2 , ..., a_m .

La recherche est désormais limitée à une liste ne contenant pas plus de $\lceil n / 2 \rceil$ éléments. (Rappeler que $\lceil x \rceil$ est le plus petit entier supérieur ou égal à x .) En utilisant la même procédure, comparez x à le milieu de la liste restreinte. Limitez ensuite la recherche à la première ou à la seconde moitié du liste. Répétez ce processus jusqu'à obtenir une liste avec un terme. Déterminez ensuite si ce terme est x . Le pseudocode de l'algorithme de recherche binaire est affiché en tant qu'algorithme 3.

ALGORITHME 3 L'algorithme de recherche binaire.

procédure *recherche binaire* (x : entier, a_1 , a_2 , ..., a_n : nombres entiers croissants)
i : = 1 { i est l'extrémité gauche de l'intervalle de recherche}
j : = n { j est l'extrémité droite de l'intervalle de recherche}
alors que *je* <*j*
  m : = $\lfloor (i + j) / 2 \rfloor$
  si x> a_m **alors** i : = m + 1
  sinon j : = m
si x = a_i **alors** *emplacement* : = i
sinon *emplacement* : = 0
emplacement de **retour** { *emplacement* est l'indice i du terme a_i égal à x , ou 0 si x n'est pas trouvé}

L'algorithme 3 procède en rétrécissant successivement la partie de la séquence cherché. A tout moment donné que les termes d' *un* $_i$ à *un* $_j$ sont à l'étude. En d'autre les mots, i et j sont respectivement les plus petits et les plus grands indices des termes restants. L'algorithme 3 continue de restreindre la partie de la séquence recherchée jusqu'à un seul terme de la séquence reste. Lorsque cela est fait, une comparaison est effectuée pour voir si ce terme est égal à x .

Tri

L'ordre des éléments d'une liste est un problème qui se produit dans de nombreux contextes. Par exemple, pour produire un annuaire téléphonique il faut alphabétiser les noms des abonnés. De même, la production un répertoire de chansons disponibles au téléchargement nécessite que leurs titres soient classés par ordre alphabétique. La mise en ordre des adresses dans une liste de diffusion par e-mail peut déterminer s'il y a des doublons adresses. Pour créer un dictionnaire utile, les mots doivent être classés par ordre alphabétique. De même, générer une liste de pièces nécessite que nous les commandions en fonction de l'augmentation du numéro de pièce.

Supposons que nous ayons une liste d'éléments d'un ensemble. De plus, supposons que nous ayons un moyen de ordonner les éléments de l'ensemble. (La notion d'ordonner des éléments d'ensembles sera discutée en détail dans Section 9.6.) Le **tri** consiste à placer ces éléments dans une liste dans laquelle les éléments sont en augmentation commande. Par exemple, le tri de la liste 7, 2, 1, 4, 5, 9 produit la liste 1, 2, 4, 5, 7, 9. Le tri du la liste d , h , c , a , f (en utilisant l'ordre alphabétique) produit la liste a , c , d , f , h .

Un pourcentage incroyablement élevé de ressources informatiques est consacré au tri d'une chose ou un autre. Par conséquent, beaucoup d'efforts ont été consacrés au développement d'algorithmes de tri. Un nombre étonnamment élevé d'algorithmes de tri ont été conçus en utilisant des stratégies avec de nouvelles introductions régulières. Dans son travail fondamental, *The Art of Computer Programmation,* Donald Knuth consacre près de 400 pages au tri, couvrant une quinzaine de pages différents algorithmes de tri en profondeur! Plus de 100 algorithmes de tri ont été développés et il est surprenant de constater à quelle fréquence de nouveaux algorithmes de tri sont développés. Parmi les les plus récents algorithmes de tri qui ont fait leur chemin sont le tri de la bibliothèque, également connu sous le nom de tri par insertion à espacement, inventé en 2006. Il existe de nombreuses raisons pour lesquelles Les algorithmes d'ingénierie intéressent les informaticiens et les mathématiciens. Parmi ces raisons figurent que certains algorithmes sont plus faciles à mettre en œuvre, certains algorithmes sont plus efficaces (soit en général, ou lorsqu'ils sont fournis avec certaines caractéristiques, telles que des listes légèrement ordre), certains algorithmes tirent parti d'architectures informatiques particulières, et certains les gorithmes sont particulièrement intelligents. Dans cette section, nous présenterons deux algorithmes de tri, le tri à bulles et le tri par insertion. Deux autres algorithmes de tri, le tri par sélection et le type d'insertion binaire, sont introduits dans les exercices, et le type de secoueur est présenté dans les Exercices supplémentaires. Dans la section 5.4, nous discuterons du tri par fusion et introduisez le tri rapide dans les exercices de cette section; le type de tournoi est présenté dans l'exercice défini à la section 11.2. Nous couvrons les algorithmes de tri à la fois parce que le tri est un problème important et parce que ces algorithmes peuvent servir d'exemples pour de nombreux concepts importants.

On pense que le tri tient le dossier comme problème résolu par le plus fondamentalement différent algorithmes!

LE TRI DES BULLES Le **tri des bulles** est l'un des algorithmes de tri les plus simples, mais pas un des plus efficaces. Il met une liste en ordre croissant en comparant successivement les éléments, en les échangeant s'ils sont dans le mauvais ordre. Pour effectuer le tri à bulles, nous effectuer l'opération de base, c'est-à-dire interchanger un élément plus grand avec un élément plus petit après il, en commençant au début de la liste, pour un laissez-passer complet. Nous répétons cette procédure jusqu'à ce que le tri soit Achevée. Le pseudocode pour le tri des bulles est donné comme algorithme 4. Nous pouvons imaginer les éléments dans la liste placée dans une colonne. Dans le tri à bulles, les petits éléments «bulle» vers le haut comme ils sont échangés avec des éléments plus grands. Les éléments plus gros «coulent» vers le bas. C'est illustré dans l'exemple 4.

EXEMPLE 4 Utilisez le tri à bulles pour mettre 3, 2, 4, 1, 5 en ordre croissant.

Premier passage					Deuxième passe		
3	2	2	2		2	2	2
2	3	3	3		3	3	1
4	4	4	1		1	1	3
1	1	1	4		4	4	4
5	5	5	5		5	5	5

Troisième passage			Quatrième passe
2	1		1
1	2		2
3	3		3
4	4		4
5	5		5

: un échange

: paire dans le bon ordre

numéros en couleur
garantie d'être en bon ordre

FIGURE 1 Les étapes d'un tri à bulles.

Solution: les étapes de cet algorithme sont illustrées à la figure 1. Commencez par comparer les deux premiers éléments, 3 et 2. Parce que 3 > 2, échange 3 et 2, produisant la liste 2 , 3 , 4 , 1 , 5. Parce que 3 < 4, continuez en comparant 4 et 1. Parce que 4 > 1, échangez 1 et 4, produisant la liste 2 , 3 , 1 , 4 , 5. Parce que 4 < 5, la première passe est terminée. La première passe garantit que le plus grand l'élément, 5, est dans la bonne position.

La deuxième passe commence par comparer 2 et 3. Parce que ceux-ci sont dans le bon ordre, 3 et 1 sont comparés. Parce que 3 > 1, ces nombres sont échangés, produisant 2 , 1 , 3 , 4 , 5. Parce que 3 < 4, ces nombres sont dans le bon ordre. Il n'est pas nécessaire de faire plus de comparaisons pour cette passe car 5 est déjà dans la bonne position. Le deuxième laissez-passer garantit que le les deux éléments les plus grands, 4 et 5, sont dans leurs positions correctes.

La troisième passe commence par comparer 2 et 1. Celles-ci sont échangées car 2> 1, produisant ing 1 , 2 , 3 , 4 , 5. Parce que 2 < 3, ces deux éléments sont dans le bon ordre. Il n'est pas nécessaire de faire d'autres comparaisons pour cette passe car 4 et 5 sont déjà dans les bonnes positions. le la troisième passe garantit que les trois éléments les plus grands, 3, 4 et 5, sont dans leurs positions correctes.

La quatrième passe consiste en une comparaison, à savoir la comparaison de 1 et 2. Parce que 1 < 2, ces éléments sont dans le bon ordre. Ceci termine le tri des bulles. ▲

ALGORITHME 4 Le tri des bulles.

procédure *bubbleort* ($a_1, ..., a_n$: nombres réels avec $n \geq 2$)
pour $i := 1$ **à** $n - 1$
  pour $j := 1$ **à** $n - i$
    si $a_j > a_{j+1}$ **alors** échangez a_j et a_{j+1}
{ $a_1, ..., a_n$ est en ordre croissant}

LE TRI D'INSERTION Le **tri par insertion** est un algorithme de tri simple, mais il est généralement pas le plus efficace. Pour trier une liste avec n éléments, le tri par insertion commence par le second élément. Le tri par insertion compare ce deuxième élément au premier élément et l'insère avant le premier élément s'il ne dépasse pas le premier élément et après le premier élément s'il dépasse le premier élément. À ce stade, les deux premiers éléments sont dans le bon ordre. Le troisième l'élément est ensuite comparé au premier élément, et s'il est plus grand que le premier élément, il est par rapport au deuxième élément; il est inséré dans la bonne position parmi les trois premiers éléments.

En général, à la j ème étape du tri par insertion, le j ème élément de la liste est inséré dans la position correcte dans la liste des j -1 éléments précédemment triés . Pour insérer le j ème élément dans la liste, une technique de recherche linéaire est utilisée (voir exercice 43); le j ème élément est successivement par rapport aux j -1 éléments déjà triés au début de la liste jusqu'au premier élément qui n'est pas inférieur à ce que cet élément est trouvé ou jusqu'à ce qu'il ait été comparé à tous les éléments j - 1; le j e L'élément est inséré dans la position correcte afin que les premiers j éléments soient triés. L'algorithme continue jusqu'à ce que le dernier élément soit placé dans la position correcte par rapport à la liste déjà triée des n - 1 premiers éléments. Le tri par insertion est décrit dans le pseudocode de l'algorithme 5.

EXEMPLE 5 Utilisez le tri par insertion pour mettre les éléments de la liste 3, 2 , 4 , 1 , 5 dans l'ordre croissant.

Solution: le tri par insertion compare d'abord 2 et 3. Parce que 3 > 2, il place 2 en première position, produire la liste 2, 3, 4 , 1 , 5 (la partie triée de la liste est affichée en couleur). À ce stade, 2 et 3 sont dans le bon ordre. Ensuite, il insère le troisième élément, 4, dans la partie déjà triée de la liste en faisant les comparaisons 4 > 2 et 4 > 3. Parce que 4 > 3 , 4 reste en troisième position. À ce stade, la liste est 2, 3, 4, 1, 5 et nous savons que l'ordre des trois premiers éléments est correct. Ensuite, nous trouvons la bonne place pour le quatrième élément, 1, parmi les déjà triés éléments, 2 , 3 , 4. Parce que 1 < 2, nous obtenons la liste 1, 2, 3, 4, 5. Enfin, nous insérons 5 dans le corriger la position en la comparant successivement à 1, 2, 3 et 4. Parce que 5 > 4, il reste à la fin de la liste, produisant l'ordre correct pour la liste entière. ▲

ALGORITHME 5 Le tri par insertion.

tri par insertion de **procédure** (a_1 , a_2 , ..., a_n : nombres réels avec $n \geq 2$)
pour j : = 2 **à** n
  i : = 1
  tandis *que* $_j$ > a_i
    i : = i + 1
  m : = a_j
  pour k : = 0 **à** j - i - 1
    a_{j-k} : = a_{j-k-1}
  a_i : = m
{ a_1 , ..., a_n est en ordre croissant}

Algorithmes gourmands

«La cupidité est bonne ... La cupidité a raison, la cupidité fonctionne. La cupidité clarifie ... »- parlé par le personnage Gordon Gecko dans le film *Wall Street.*

De nombreux algorithmes que nous étudierons dans ce livre sont conçus pour résoudre **des problèmes d'optimisation** . Le but de ces problèmes est de trouver une solution au problème donné qui minimise ou maximise la valeur d'un paramètre. Les problèmes d'optimisation étudiés plus loin dans ce texte incluent trouver un itinéraire entre deux villes avec le plus petit kilométrage total, déterminer un moyen de coder messages utilisant le moins de bits possible et recherche d'un ensemble de liaisons fibre entre les nœuds du réseau en utilisant le moins de fibres.

Vous devez prouver qu'un algorithme gourmand toujours trouve une solution optimale.

Étonnamment, l'une des approches les plus simples conduit souvent à une solution d'optimisation problème. Cette approche sélectionne le meilleur choix à chaque étape, au lieu de considérer toutes les séquences des étapes qui peuvent conduire à une solution optimale. Des algorithmes qui font ce qui semble être le «meilleur» choix à chaque étape sont appelés **algorithmes gourmands** . Une fois que nous savons qu'un algorithme gourmand trouve un solution réalisable, nous devons déterminer si elle a trouvé une solution optimale. (Notez que nous appeler l'algorithme «gourmand», qu'il trouve ou non une solution optimale.) Pour ce faire, soit nous prouvons que la solution est optimale ou nous montrons qu'il y a un contre-exemple où l'algorithme donne une solution non optimale. Pour rendre ces concepts plus concrets, nous considérerons un algorithme qui fait le changement en utilisant des pièces.

EXEMPLE 6 Considérons le problème de la modification de n cents avec les quartiers, les dix sous, les nickels et les sous, et en utilisant le moins de pièces au total. Nous pouvons concevoir un algorithme gourmand pour faire des changements pour n cents en faisant un choix localement optimal à chaque étape; c'est-à-dire qu'à chaque étape, nous choisissons la pièce de la plus grande dénomination possible à ajouter à la pile de monnaie sans dépasser n cents. Pour Par exemple, pour effectuer un changement de 67 cents, nous sélectionnons d'abord un trimestre (en laissant 42 cents). Nous sélectionnons ensuite un deuxième trimestre (laissant 17 cents), suivi d'un centime (laissant 7 cents), suivi d'un nickel (laissant 2 cents), suivi d'un sou (laissant 1 cent), suivi d'un sou. ▲

Nous affichons un algorithme de changement gourmand pour n cents, en utilisant n'importe quel ensemble de dénominations de pièces, comme l'algorithme 6.

ALGORITHME 6 Algorithme gourmand de changement.

changement de **procédure** (c_1 , c_2 , ..., c_r : valeurs des dénominations des pièces, où $c_1 > c_2 > \cdots > c_r$; n : un entier positif)
pour i : = 1 **à** r
  d_i : = 0 { d_i compte les pièces de monnaie c_i utilisées}
  tandis que $n \geq c_i$
    d_i : = d_i + 1 {ajouter une pièce de monnaie c_i }
    n : = n - c_i
{ d_i est le nombre de pièces de dénomination c_i dans la variation pour i = 1 , 2 , ..., r }

Nous avons décrit un algorithme gourmand pour effectuer des changements en utilisant un ensemble fini de pièces avec dénominations c_1 , c_2 , ..., c_r . Dans le cas particulier où les quatre dénominations sont des trimestres dimes, nickels et penny, nous avons $c_1 = 25$, $c_2 = 10$, $c_3 = 5$ et $c_4 = 1$. Pour ce cas, nous montrera que cet algorithme conduit à une solution optimale dans le sens où il utilise le moins pièces possibles. Avant de commencer notre preuve, nous montrons qu'il existe des ensembles de pièces pour lesquels l'algorithme gourmand (algorithme 6) ne produit pas nécessairement de changement en utilisant le moins de pièces possible. Par exemple, si nous n'avons que des quarts, des dix sous et des sous (et pas de nickels) à utiliser, l'algorithme gourmand ferait un changement de 30 cents en utilisant six pièces - un quart et cinq centimes, alors que nous aurions pu utiliser trois pièces, à savoir trois sous.

LEMMA 1 Si n est un entier positif, alors n cents en variation en utilisant les quarts, les dix sous, les nickels et les sous utiliser le moins de pièces possible a au plus deux dimes, au plus un nickel, au plus quatre centimes, et ne peut pas avoir deux centimes et un nickel. La quantité de changement en dix sous, nickels, et les sous ne peuvent pas dépasser 24 cents.

Preuve: Nous utilisons une preuve par contradiction. Nous montrerons que si nous avions plus que le nombre spécifié nombre de pièces de chaque type, nous pourrions les remplacer en utilisant moins de pièces de même valeur. Nous notons que si nous avions trois dimes, nous pourrions les remplacer par un quart et un nickel, si nous avait deux nickels, nous pourrions les remplacer par un centime, si nous avions cinq centimes, nous pourrions remplacer les avec un nickel, et si nous avions deux dimes et un nickel, nous pourrions les remplacer par un quart. Parce que nous pouvons avoir au plus deux sous, un nickel et quatre sous, mais nous ne pouvons pas en avoir deux dix sous et un nickel, il s'ensuit que 24 cents est le plus d'argent que nous pouvons avoir en dix sous, nickels, et quelques centimes lorsque nous apportons des modifications en utilisant le moins de pièces pour n cents.

THÉORÈME 1 L'algorithme gourmand (algorithme 6) produit le changement en utilisant le moins de pièces possible.

Preuve: Nous utiliserons une preuve par contradiction. Supposons qu'il existe un entier positif n tel que il existe un moyen de faire des changements pour n cents en utilisant des quarts, des dix sous, des nickels et des centimes qui utilise moins de pièces que l'algorithme gourmand n'en trouve. On note d'abord que q, le nombre de trimestres utilisés de cette façon optimale pour effectuer des changements pour n cents, doit être le même que q, le nombre de trimestres utilisé par l'algorithme gourmand. Pour le montrer, notons d'abord que l'algorithme gourmand utilise le plus quart possible, donc $q \leq q$. Cependant, il est également vrai que q ne peut pas être inférieur à q. Si c'était, nous aurions besoin de compenser au moins 25 cents avec des sous, des nickels et des sous dans cet optimal façon de faire le changement. Mais cela est impossible par le lemme 1.

Parce qu'il doit y avoir le même nombre de trimestres dans les deux façons d'apporter des changements, le la valeur des dix sous, des nickels et des sous de ces deux façons doit être la même, et ces pièces ne valent pas plus de 24 cents. Il doit y avoir le même nombre de dix sous, car les gourmands algorithme utilisé le plus de dimes possible et par le lemme 1, lorsque le changement est effectué en utilisant le moins pièces de monnaie possibles, au plus un nickel et au plus quatre sous sont utilisés, de sorte que le plus de dix sous possible sont également utilisés de la manière optimale pour apporter des changements. De même, nous avons le même numéro de nickels et, enfin, le même nombre de centimes.

Un algorithme gourmand fait le meilleur choix à chaque étape selon un critère spécifié. L'exemple suivant montre qu'il peut être difficile de déterminer lequel des nombreux critères possibles choisir.

EXEMPLE 7 Supposons que nous ayons un groupe de discussions proposées avec des heures de début et de fin prédéfinies Concevoir un gourmand algorithme pour programmer autant de ces conférences que possible dans une salle de conférence, sous les hypothèses qu'une fois qu'une conversation commence, elle se poursuit jusqu'à la fin, deux conversations ne peuvent pas se dérouler en même temps, et une conversation peut commencer en même temps qu'une autre se termine. Supposons que la conversation j commence à l'instant s_j (où s signifie *début*) et se termine à l'instant e_j (où e signifie *fin*).

Solution: Pour utiliser un algorithme gourmand pour planifier le plus de conversations, c'est-à-dire un calendrier optimal, nous besoin de décider comment choisir le discours à ajouter à chaque étape. Il existe de nombreux critères que nous pourrions utiliser pour sélectionner un exposé à chaque étape, où nous avons choisi parmi les exposés qui ne se chevauchent pas déjà choisi. Par exemple, nous pourrions ajouter des discussions dans l'ordre de début le plus tôt, nous pourrions ajouter des conversations dans ordre de temps le plus court, nous pourrions ajouter des discussions dans l'ordre du temps de fin le plus tôt, ou nous pourrions utiliser certains autre critère.

Nous considérons maintenant ces critères possibles. Supposons que nous ajoutons le discours qui commence le plus tôt parmi les entretiens compatibles avec ceux déjà sélectionnés. Nous pouvons construire un contre-exemple pour voir que l'algorithme résultant ne produit pas toujours un calendrier optimal. Par exemple, supposons que nous avons trois conférences: la conférence 1 commence à 8 heures et se termine à midi, la conférence 2 commence à 9 heures et se termine à 10 h 00 et Talk 3 commence à 11 h 00 et se termine à 12 h 00. Nous sélectionnons d'abord le Talk 1 car il commence plus tôt. Mais une fois que nous avons sélectionné Talk 1, nous ne pouvons pas sélectionner Talk 2 ou Talk 3 car les deux se chevauchent Talk 1. Par conséquent, cet algorithme gourmand ne sélectionne qu'un seul talk. Ce n'est pas optimal car nous pourrions programmer Talk 2 et Talk 3, qui ne se chevauchent pas.

Supposons maintenant que nous ajoutions le discours le plus court parmi les pourparlers qui ne chevauchent aucun de ceux déjà sélectionné. Encore une fois, nous pouvons construire un contre-exemple pour montrer que cet algorithme gourmand ne produit pas toujours un horaire optimal. Supposons donc que nous ayons trois discussions: la conversation 1 commence à 8 h et se termine à 9 h 15, Talk 2 commence à 9 h et se termine à 10 h et Talk 3 commence à 9 h 45 et se termine à 11 h. Nous sélectionnons Talk 2 car il est le plus court et nécessite une heure. Une fois que nous sélectionnons Talk 2, nous ne pouvons pas sélectionner Talk 1 ou Talk 3 car aucun n'est compatible avec Talk 2. Par conséquent, cet algorithme gourmand ne sélectionne qu'un seul talk. Cependant, il est possible de sélectionner deux conversations, Talk 1 et Talk 3, qui sont compatibles.

Cependant, il peut être démontré que nous programmons le plus de conversations possibles si à chaque étape nous sélectionnons la conversation avec l'heure de fin la plus rapprochée parmi les conversations compatibles avec celles déjà sélectionnées. Nous le prouverons au chapitre 5 en utilisant la méthode d'induction mathématique. La première étape, nous va faire est de trier les discussions en fonction de l'augmentation de l'heure de fin. Après ce tri, nous réétiquetons les pourparlers de sorte que $e_1 \leq e_2 \leq \ldots \leq e_n$. L'algorithme gourmand résultant est donné comme algorithme 7. ▲

ALGORITHM 7 Algorithme gourmand pour la planification des entretiens.

calendrier de la **procédure** ($s_1 \leq s_2 \leq \cdots \leq s_n$: heures de début des conversations,
$e_1 \leq e_2 \leq \cdots \leq e_n$: heures de fin des discussions)

trier les conversations par heure de fin et réorganiser de telle sorte que $e_1 \leq e_2 \leq \ldots \leq e_n$
$S := \emptyset$

pour $j := 1$ **à** n

si talk j est compatible avec S **alors**
$S := S \cup$ {parler j }
return S { S est l'ensemble des discussions programmées}

Le problème de l'arrêt

Nous allons maintenant décrire une preuve de l'un des théorèmes les plus célèbres de l'informatique.Nous allons montrent qu'il existe un problème qui ne peut pas être résolu à l'aide d'une procédure.Autrement dit, nous allons montrer il y a des problèmes insolubles. Le problème que nous étudierons est le **problème de** l' **arrêt** . Il demande si il existe une procédure qui fait cela: il prend en entrée un programme informatique et une entrée dans le programme et détermine si le programme s'arrêtera éventuellement lors de l'exécution avec cette entrée.Ce serait pratique d'avoir une telle procédure, si elle existait. Certes, pouvoir tester si un programme entré dans une boucle infinie serait utile lors de l'écriture et du débogage de programmes.cependant, en 1936, Alan Turing a montré qu'aucune procédure de ce type n'existe (voir sa biographie dans la section 13.4).

Avant de présenter une preuve que le problème d'arrêt est insoluble, notons d'abord que nous ne pouvons pas exécutez simplement un programme et observez ce qu'il fait pour déterminer s'il se termine lors de l'exécution avec l'entrée donnée. Si le programme s'arrête, nous avons notre réponse, mais s'il continue à fonctionner après une durée fixe s'est écoulée, nous ne savons pas si cela ne s'arrêtera jamais ou si nous ne l'avons tout simplement pas attendez assez longtemps pour qu'il se termine. Après tout, il n'est pas difficile de concevoir un programme qui s'arrêtera ce n'est qu'au bout de plus d'un milliard d'années.

Nous décrirons la preuve de Turing que le problème d'arrêt est insoluble;c'est une preuve par contradiction. (Le lecteur doit noter que notre preuve n'est pas complètement rigoureuse, car nous n'ont pas explicitement défini ce qu'est une procédure. Pour y remédier, le concept de machine de Turing est nécessaire. Ce concept est présenté à la section 13.5.)

Preuve: Supposons qu'il existe une solution au problème d'arrêt, une procédure appelée $H (P, I)$. le la procédure $H (P, I)$ prend deux entrées, l'une un programme P et l'autre I , une entrée au programme P . $H (P, I)$ génère la chaîne «stop» en sortie si H détermine que P s'arrête lorsqu'il est donné I comme contribution. Sinon, $H (P, I)$ génère la chaîne «boucles pour toujours» en sortie. Nous allons maintenant dériver un contradiction.

Lorsqu'une procédure est codée, elle est exprimée sous la forme d'une chaîne de caractères;cette chaîne peut être interprété comme une séquence de bits. Cela signifie qu'un programme lui-même peut être utilisé comme données. Donc un programme peut être considéré comme une entrée vers un autre programme, ou même lui-même. Par conséquent, H peut prendre un programme P comme ses deux entrées, qui sont un programme et une entrée dans ce programme. H devrait être capable de déterminer si P s'arrêtera quand on lui donnera une copie de lui-même en entrée.

Pour montrer qu'aucune procédure H n'existe qui résout le problème d'arrêt, nous construisons un simple procédure $K (P)$, qui fonctionne comme suit, en utilisant la sortie $H (P, P)$. Si la sortie de $H (P, P)$ est «boucle pour toujours», ce qui signifie que P boucle pour toujours lorsqu'il reçoit une copie de lui-même en tant que entrée, puis $K (P)$ s'arrête. Si la sortie de $H (P, P)$ est «arrêt», ce qui signifie que P s'arrête lorsqu'il est donné une copie de lui-même en entrée, puis $K (P)$ boucle pour toujours. Autrement dit, $K (P)$ fait le contraire de ce que le sortie de $H (P, P)$ spécifie. (Voir figure 2.)

Supposons maintenant que nous fournissons K comme entrée à K . On note que si la sortie de $H (K, K)$ est «boucles pour toujours », puis par la définition de $K,$ nous voyons que $K (K)$ s'arrête. Sinon, si la sortie de $H (K, K)$

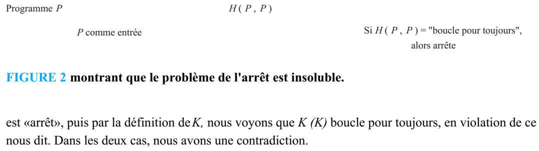


FIGURE 2 **montrant que le problème de l'arrêt est insoluble.**

est «arrêt», puis par la définition de $K,$ nous voyons que $K (K)$ boucle pour toujours, en violation de ce que H nous dit. Dans les deux cas, nous avons une contradiction.

Ainsi, H ne peut pas toujours donner les bonnes réponses. Par conséquent, aucune procédure résout le problème d'arrêt.

Des exercices

1. Énumérez toutes les étapes utilisées par l'algorithme 1 pour trouver le maximum de la liste 1, 8, 12, 9, 11, 2, 14, 5, 10, 4.

2. Déterminez quelles caractéristiques d'un algorithme décrit dans le texte (après l'algorithme 1) le programme suivant

3. Décrire un algorithme qui prend en entrée une liste de n distincts entiers tincts et trouve l'emplacement du plus grand même entier dans la liste ou renvoie 0 s'il n'y a pas d'entiers pairs dans la liste.

cédures ont et qui leur manquent.

a) procédure *double* (n : entier positif)
  tandis que $n > 0$
    $n := 2n$

b) *division de la* **procédure** (n : entier positif)
  tandis que $n \geq 0$
    $m := 1 / n$
    $n := n - 1$

c) *somme de* **procédure** (n : entier positif)
  somme : = 0
  alors que *je* < 10
    somme : = *somme* + *i*

d) procédure *choisir* (a , b : entiers)
  $x := a$ ou b

3. Concevoir un algorithme qui trouve la somme de tous les entiers dans une liste.

4. Décrire un algorithme qui prend en entrée une liste de n intère et produit en sortie la plus grande différence obmaintenu en soustrayant un entier de la liste de celui le suivre.

5. Décrivez un algorithme qui prend en entrée une liste de n nombres dans un ordre non décroissant et produit la liste de tous les valeurs qui se produisent plusieurs fois. (Rappelons qu'une liste de les nombres entiers ne **diminuent pas** si chaque nombre entier dans la liste est à au moins aussi grand que l'entier précédent dans la liste.)

6. décrire un algorithme qui prend en entrée une liste de n integers et trouve le nombre d'entiers négatifs dans le liste.

7. Décrire un algorithme qui prend en entrée une liste de n nombres gers et trouve l'emplacement du dernier entier pair dans le list ou renvoie 0 s'il n'y a pas d'entiers pairs dans la liste.

9. Un **palindrome** est une chaîne qui se lit de la même façon et en arrière. Décrire un algorithme pour déterminer si une chaîne de n caractères est un palindrome.

10. Concevoir un algorithme pour calculer x^n , où x est un réel nombre et n est un entier. [*Astuce:* Donnez d'abord une procédure pour calculer x^n quand n est non négatif par successives multiplication par x , en commençant par 1. Ensuite, étendez ce procédure, et utiliser le fait que $x^{-n} = 1 / x^n$ calculer x^n quand n est négatif.]

11. Décrire un algorithme qui échange les valeurs de la variables x et y , en utilisant uniquement des affectations. Quel est le nombre minimum d'énoncés d'affectation nécessaires à faire cette?

12. Décrivez un algorithme qui utilise uniquement les états qui remplace le triple (x, y, z) par (y, z, x) . Quel est le nombre minimum de déclarations d'affectation nécessaire?

13. Énumérez toutes les étapes utilisées pour rechercher 9 dans la séquence 1, 3, 4, 5, 6, 8, 9, 11 en utilisant

a) une recherche linéaire. **b)** une recherche binaire.

14. Énumérez toutes les étapes utilisées pour rechercher 7 dans la séquence indiquée dans l'exercice 13 pour une recherche linéaire et une recherche binaire.

15. Décrivez un algorithme qui insère un entier x dans l'application position appropriée dans la liste $a_1, a_2, ..., a_n$ d'entiers qui sont en ordre croissant.

16. Décrire un algorithme pour trouver le plus petit entier dans une séquence finie de nombres naturels.

17. Décrire un algorithme qui localise la première occurrence de le plus grand élément d'une liste finie d'entiers, où le les entiers de la liste ne sont pas nécessairement distincts.

18. Décrire un algorithme qui localise la dernière occurrence de le plus petit élément d'une liste finie d'entiers, où le les entiers de la liste ne sont pas nécessairement distincts.

Page 224

19. Décrivez un algorithme qui produit le maximum, dian, moyenne et minimum d'un ensemble de trois entiers. (Le **la médiane** d'un ensemble d'entiers est l'élément central de la liste lorsque ces entiers sont répertoriés par ordre croissant de taille. La **moyenne** d'un ensemble d'entiers est la somme des entiers divisé par le nombre d'entiers dans l'ensemble.)

20. Décrire un algorithme pour trouver à la fois le plus grand et le les plus petits entiers dans une séquence finie d'entiers.

21. Décrire un algorithme qui met les trois premiers termes de une séquence d'entiers de longueur arbitraire en augmentant commande.

22. Décrire un algorithme pour trouver le mot le plus long dans un phrase glish (où une phrase est une séquence de symboles, soit une lettre ou un blanc, qui peut ensuite être divisé en alternance de mots et de blancs).

23. Décrire un algorithme qui détermine si une fonction d'un ensemble fini d'entiers à un autre ensemble fini d'entiers est sur.

24. Décrire un algorithme qui détermine si une fonction d'un ensemble fini à un autre ensemble fini est un à un.

25. Décrivez un algorithme qui comptera le nombre de 1 dans une chaîne de bits en examinant chaque bit de la chaîne pour déterminer le mien que ce soit un 1 bit.

26. Changez l'algorithme 3 pour que la procédure de recherche binaire compare x à *un* $_m$ à chaque étape de l'algorithme, avec le algorithme se terminant si $x = a_m$. Quel avantage cette version de l'algorithme?

27. L' **algorithme de recherche ternaire** localise un élément dans une liste d'augmenter les nombres entiers en divisant successivement la liste en trois sous-listes égales (ou aussi proches que possible) taille, et restreindre la recherche à la pièce appropriée. Spécifiez les étapes de cet algorithme.

28. Spécifiez les étapes d'un algorithme qui localise un élément dans une liste d'entiers croissants en se divisant successivement la liste en quatre sous-listes d'égale (ou aussi proche d'égale que possible) et en limitant la recherche à la taille appropriée pièce.

33. Concevoir un algorithme qui trouve le premier terme d'une séquence d'entiers positifs inférieurs à la valeur immédiatement antérieure terme sortant de la séquence.

34. Utilisez le tri à bulles pour trier 6, 2, 3, 1, 5, 4, en listes obtenues à chaque étape.

35. Utilisez le tri à bulles pour trier 3, 1, 5, 7, 4, en affichant les listes obtenu à chaque étape.

36. Utilisez le tri à bulles pour trier d , f , k , m , a , b , en montrant listes obtenues à chaque étape.

∗ 37. Adapter l'algorithme de tri à bulles pour qu'il s'arrête lorsque aucun échange n'est requis. Exprimez cela plus efficacement version de l'algorithme en pseudocode.

38. Utilisez le tri par insertion pour trier la liste de l'exercice 34, des listes obtenues à chaque étape.

39. Utilisez le tri par insertion pour trier la liste de l'exercice 35, des listes obtenues à chaque étape.

40. Utilisez le tri par insertion pour trier la liste de l'exercice 36, des listes obtenues à chaque étape.

Le **tri de sélection** commence par trouver le moindre élément dans le liste. Cet élément est déplacé vers l'avant. Alors le moindre élément parmi les éléments restants est trouvé et mis dans le deuxième position. Cette procédure est répétée jusqu'à ce que la liste entière a été trié.

41. Triez ces listes en utilisant le tri par sélection.

a) 3, 5, 4, 1, 2 **b)** 5, 4, 3, 2, 1
c) 1, 2, 3, 4, 5

42. Écrivez l'algorithme de tri de sélection en pseudocode.

43. Décrire un algorithme basé sur la recherche linéaire de définissant la position correcte dans laquelle insérer un nouveau élément dans une liste déjà triée.

44. Décrire un algorithme basé sur la recherche binaire de définissant la position correcte dans laquelle insérer un nouveau élément dans une liste déjà triée.

45. Combien de comparaisons le tri par insertion utilise-t-il pour trier la liste $1, 2, ..., n$?

46. Combien de comparaisons le tri par insertion utilise-t-il pour trier la liste $n, n - 1, ..., 2, 1$?

Dans une liste d'éléments, le même élément peut apparaître plusieurs fois. Un **mode** d'une telle liste est un élément qui se produit au moins aussi souvent que chacun des autres éléments; une liste a plus de un mode lorsque plusieurs éléments apparaissent au maximum nombre de fois.

29. Concevoir un algorithme qui trouve un mode dans une liste de plier des entiers. (Rappelons qu'une liste d'entiers n'est pas augmente si chaque terme est au moins aussi grand que le précédent terme.)

30. Concevez un algorithme qui trouve tous les modes. (Rappelons qu'un la liste des entiers ne diminue pas si chaque terme de la liste est au moins aussi grand que le terme précédent.)

31. Concevez un algorithme qui trouve le premier terme d'une séquence d'entiers qui équivaut à un terme précédent du séquence.

32. Concevoir un algorithme qui trouve tous les termes d'une séquence finie de nombres entiers supérieurs à la somme de tous termes précédents de la séquence.

Le **tri par insertion binaire** est une variation du tri par insertion qui utilise une technique de recherche binaire (voir exercice 44) plutôt qu'une technique de recherche linéaire pour insérer le i ème élément dans le place correcte parmi les éléments précédemment triés.

47. Afficher toutes les étapes utilisées par le tri par insertion binaire pour trier la liste 3, 2, 4, 5, 1, 6.

48. Comparez le nombre de comparaisons utilisées par tri et le tri par insertion binaire pour trier la liste 7, 4, 3, 8, 1, 5, 4, 2.

∗ **49.** Exprimez le tri par insertion binaire en pseudocode.

50. a) Concevoir une variante du type d'insertion qui utilise une technique de recherche d'oreille qui insère le j ème élément dans le place correcte en la comparant d'abord avec la $(j - 1)$ m élément, puis le $(j - 2)$ ème élément si nécessaire, et bientôt.

b) Utilisez votre algorithme pour trier 3, 2, 4, 5, 1, 6.

c) Répondez à l'exercice 45 en utilisant cet algorithme.

d) Répondez à l'exercice 46 en utilisant cet algorithme.

51. Lorsqu'une liste d'éléments est proche de l'ordre correct, serait-il préférable d'utiliser un tri par insertion ou sa variation décrit dans l'exercice 50?

52. Utilisez l'algorithme gourmand pour faire des changements en utilisant des quarts, dix sous, nickels et sous pour

a) 87 cents. **b)** 49 cents.
c) 99 cents. **d)** 33 cents.

53. Utilisez l'algorithme gourmand pour faire des changements en utilisant des quarts, dix sous, nickels et sous pour

a) 51 cents. **b)** 69 cents.
c) 76 cents. **d)** 60 cents.

54. Utilisez l'algorithme gourmand pour faire des changements en utilisant tres, dix sous et quelques centimes (mais pas de nickels) pour chacun des montants indiqués à l'exercice 52. Pour lequel de ces montants l'algorithme gourmand utilise-t-il le moins de pièces de ces dénominations possibles?

55. Utilisez l'algorithme gourmand pour faire des changements en utilisant tres, dix sous et quelques centimes (mais pas de nickels) pour chacun des montants indiqués à l'exercice 53. Pour lequel de ces montants l'algorithme gourmand utilise-t-il le moins de pièces de ces dénominations possibles?

56. Montrez que s'il y avait une pièce de 12 cents, le gourmand algorithme utilisant des quarts, des pièces de 12 cents, des dimes, des nickels, et les sous ne produiraient pas toujours le changement en utilisant le le moins de pièces possible.

57. Utilisez l'algorithme 7 pour planifier le plus grand nombre de conversations dans une salle de conférence à partir d'un ensemble proposé de conférences, si le début et les heures de fin des pourparlers sont 9h00 et 9h45;
9h30 et 10h00; 9 h 50 et 10 h 15;
10 h 00 et 10 h 30; 10 h 10 et 10 h 25;
10h30 et 10h55; 10 h 15 et 10 h 45;
10h30 et 11h00; 10 h 45 et 11 h 30;
10 h 55 et 11 h 25; 11 h 00 et 11 h 15

58. Montrer qu'un algorithme gourmand qui planifie les discussions dans un comme décrit dans l'exemple 7, en sélectionnant à chaque fois intensifier le discours qui chevauche le moins d'autres pourparlers, ne toujours produire un horaire optimal.

∗ **59. a)** Concevoir un algorithme gourmand qui détermine le moins salles de conférence nécessaires pour accueillir n entretiens étant donné le heure de début et de fin de chaque exposé.

b) Prouvez que votre algorithme est optimal.

Supposons que nous ayons s hommes $m_1, m_2, ..., m_s$ et s femmes $w_1, w_2, ..., w_s$. Nous souhaitons faire correspondre chaque personne avec un membre du sexe opposé. De plus, supposons que chaque personne rangs, par ordre de préférence, sans liens, le peuple de la le genre opposé. Nous disons qu'un appariement de personnes d'en face les sexes pour former des couples est **stable** si nous ne pouvons pas trouver un homme m et une femme w qui ne sont pas affectées les unes aux autres de telle sorte que m préfère w son partenaire affecté et w préfère m à son partenaire assigné.

60. Supposons que nous ayons trois hommes m_1, m_2 et m_3 et trois femmes w_1, w_2 et w_3. De plus, supposons que le classement préférentiel des hommes pour les trois femmes, du plus haut au plus bas, sont $m_1: w_3, w_1, w_2$; $m_2: w_1, w_2, w_3$; $m_3: w_2, w_3, w_1$; et le classement préférentiel des femmes pour les trois hommes, du plus haut au plus bas, sont $w_1: m_1, m_2, m_3$; $w_2: m_2, m_1, m_3$; $w_3: m_3, m_2, m_1$. Pour chacun des six correspondances possibles d'hommes et de femmes pour former trois couples, déterminez si cette correspondance est stable.

L' **algorithme d'acceptation différée** , également connu sous le **nom de Algorithme de Shapley** , peut être utilisé pour construire une correspondance stable des hommes et des femmes. Dans cet algorithme, les membres d'un sexe sont les **prétendants** et les membres de l'autre sexe les **suites** . L'algorithme utilise une séquence de tours; à chaque tour tous les demandeur dont la proposition a été rejetée lors du cycle pose à sa suite au rang le plus élevé qui n'a pas déjà a rejeté une proposition de ce prétendant. Une suite rejette tout Positions sauf que du prétendant que cette suite se classe au premier rang parmi tous les prétendants qui ont proposé cette suite dans ce tour ou tours précédents. La proposition de ce plus haut classement prétendant reste en suspens et est rejeté dans un tour ultérieur si un plus prétendant appelant propose dans ce tour. La série de tours se termine lorsque chaque prétendant a exactement une proposition en attente. Tout les propositions en attente sont ensuite acceptées.

61. Écrivez l'algorithme d'acceptation différée en pseudocode.

62. Montrer que l'algorithme d'acceptation différée se termine.

∗ **63.** Montrer que l'acceptation différée se termine toujours par une mission stable.

64. Montrer que le problème de déterminer si un programme avec une entrée donnée imprime jamais le chiffre 1 est insoluble.

65. Montrez que le problème suivant est résoluble. Étant donné deux programmes avec leurs contributions et la connaissance que exactement l'un d'eux s'arrête, déterminez lequel s'arrête.

66. Montrer que le problème de décider si un programme avec une entrée spécifique s'arrête est résoluble.

La croissance des fonctions

introduction

Dans la section 3.1, nous avons discuté du concept d'un algorithme. Nous avons introduit des algorithmes qui résolvent un une variété de problèmes, y compris la recherche d'un élément dans une liste et le tri d'une liste. Dans la section 3.3

nous étudierons le nombre d'opérations utilisées par ces algorithmes. En particulier, nous allons estimer le nombre de comparaisons utilisées par les algorithmes de recherche linéaire et binaire pour trouver un élément dans une séquence de n éléments. Nous allons également estimer le nombre de comparaisons utilisées par le

tri à bulles et par le tri par insertion pour trier une liste de n éléments. Le temps nécessaire pour résoudre un problème dépend de plus que le nombre d'opérations qu'il utilise. Le temps dépend aussi sur le matériel et les logiciels utilisés pour exécuter le programme qui implémente l'algorithme.cependant, lorsque nous changeons le matériel et les logiciels utilisés pour implémenter un algorithme, nous pouvons étroitement approximer le temps nécessaire pour résoudre un problème de taille n en multipliant le temps précédent requis par une constante. Par exemple, sur un supercalculateur, nous pourrions être en mesure de résoudre un problème de taille n un million de fois plus rapide que nous pouvons sur un PC.Cependant, ce facteur d'un million ne dépend pas de n (sauf peut-être de façon mineure). L'un des avantages de l'utilisation de **big- *O* notation** , que nous introduisons dans cette section, est que nous pouvons estimer la croissance d'une fonction sans se soucier des multiplicateurs constants ou des termes de commande plus petits.Cela signifie que l'utilisation de *O* notation, nous n'avons pas à nous soucier du matériel et des logiciels utilisés pour implémenter un algorithme. De plus, en utilisant la notation big- *O* , nous pouvons supposer que les différentes opérations utilisées dans un algorithme prennent le même temps, ce qui simplifie considérablement l'analyse.

La notation Big- *O* est largement utilisée pour estimer le nombre d'opérations qu'un algorithme utilise à mesure que son entrée augmente. A l'aide de cette notation, nous pouvons déterminer s'il est pratique de utilisez un algorithme particulier pour résoudre un problème à mesure que la taille de l'entrée augmente.En outre, en utilisant la notation big- *O* , nous pouvons comparer deux algorithmes pour déterminer lequel est plus efficace que la taille de l'entrée augmente. Par exemple, si nous avons deux algorithmes pour résoudre un problème, un en utilisant $100n^2 + 17n + 4$ opérations et l'autre en utilisant n^3 opérations, la notation big- *O* peut aider nous voyons que le premier algorithme utilise beaucoup moins d'opérations lorsque n est grand, même s'il utilise plus opérations pour les petites valeurs de n , telles que $n = 10$.

Cette section présente la notation big- *O* et les notations big-Omega et big-Theta associées. Nous expliquerons comment les estimations big- *O,* big-Omega et big-Theta sont construites et établies estimations de certaines fonctions importantes utilisées dans l'analyse des algorithmes.

Notation Big- *O*

La croissance des fonctions est souvent décrite à l'aide d'une notation spéciale.La définition 1 décrit cela notation.

DÉFINITION 1 Soit f et g *des* fonctions de l'ensemble des entiers ou de l'ensemble des nombres réels à l'ensemble des réels Nombres. On dit que $f(x)$ est $O(g(x))$ s'il y a des constantes C et k telles que

$$|f(x)| \leq C|g(x)|$$

chaque fois que $x > k$. [Ceci est lu comme "$f(x)$ est grand-oh de $g(x)$."]

Remarque: Intuitivement, la définition que $f(x)$ est $O(g(x))$ dit que $f(x)$ croît plus lentement que certains multiple fixe de $g(x)$ lorsque x croît sans limite.

Les constantes C et k dans la définition de la notation big- *O* sont appelées **témoins** de la la relation $f(x)$ est $O(g(x))$. Pour établir que $f(x)$ est $O(g(x))$, nous avons besoin d'une seule paire de témoins de cette relation. Autrement dit, pour montrer que $f(x)$ est $O(g(x))$, nous devons trouver *une* seule paire des constantes C et k , les témoins, tels que $|f(x)| \leq C|g(x)|$ chaque fois que $x > k$.

Notez que lorsqu'il y a une paire de témoins de la relation $f(x)$ est $O(g(x))$, il y a *infiniment de* paires de témoins. Pour voir cela, notez que si C et k sont une paire de témoins, alors toute paire C et k , où $C < C$ et $k < k$, est aussi une paire de témoins, car $|f(x)| \leq C|g(x)| \leq C|g(x)|$ chaque fois que $x > k > k$.

L'HISTOIRE DE BIG - *O* NOTATION Big- O notation a été utilisé en mathématiques pour plus d'un siècle. En informatique, il est largement utilisé dans l'analyse des algorithmes, comme sera vu dans la section 3.3. Le mathématicien allemand Paul Bachmann a d'abord présenté big-O notation en 1892 dans un livre important sur la théorie des nombres.Le grand symbole O est parfois appelé un **symbole Landau d'** après le mathématicien allemand Edmund Landau, qui a utilisé cette notation tout au long de son travail.L'utilisation de la notation big- O en informatique a été popularisée par Donald Knuth, qui a également introduit les grandes et grandes notations définies plus loin dans cette section.

TRAVAIL AVEC LA DÉFINITION DU BIG - *O* NOTATION Une approche utile pour Rechercher-ing une paire de témoins est de sélectionner d'abord une valeur de k pour laquelle la taille de $|f(x)|$ peut être facilement estimée lorsque $x > k$ et pour voir si nous pouvons utiliser cette estimation pour trouver une valeur de C pour laquelle $|f(x)| \leq C|g(x)|$ pour $x > k$. Cette approche est illustrée dans l'exemple 1.

EXEMPLE 1 Montrer que $f(x) = x^2 + 2x + 1$ est $O(x^2)$.

Solution: Nous observons que nous pouvons facilement estimer la taille de $f(x)$ lorsque $x > 1$ car $x < x^2$ et $1 < x^2$ lorsque $x > 1$. Il s'ensuit que

$$0 \leq x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$$

chaque fois que $x > 1$, comme le montre la figure 1. Par conséquent, nous pouvons prendre $C = 4$ et $k = 1$ comme témoins pour montrer que $f(x)$ est $O(x^2)$. Autrement dit, $f(x) = x^2 + 2x + 1 < 4x^2$ chaque fois que $x > 1$. (Notez qu'il il n'est pas nécessaire d'utiliser des valeurs absolues ici car toutes les fonctions dans ces égalités sont positives lorsque x est positif.)

Alternativement, nous pouvons estimer la taille de $f(x)$ lorsque $x > 2$. Lorsque $x > 2$, nous avons $2x \leq x^2$ et $1 \leq x^2$. Par conséquent, si $x > 2$, nous avons

$$0 \leq x^2 + 2x + 1 \leq x^2 + x^2 + x^2 = 3x^2.$$

Il s'ensuit que $C = 3$ et $k = 2$ sont également témoins de la relation $f(x)$ est $O(x^2)$.

$4x^2$ $x^2 + 2x + 1$ x^2

4

3

La partie du graphique de $f(x) = x^2 + 2x + 1$ qui satisfait $f(x) < 4x^2$ est indiqué en bleu.

2

1 $x^2 + 2x + 1 < 4x^2$ pour $x > 1$

1 2

FIGURE 1 La fonction $x^2 + 2x + 1$ est $O(x^2)$.

Notez que dans la relation « $f(x)$ est $O(x^2)$ », x^2 peut être remplacé par n'importe quelle fonction avec des valeurs supérieures à x^2 . Par exemple, $f(x)$ est $O(x^3)$, $f(x)$ est $O(x^2 + x + 7)$, etc.

Il est également vrai que x^2 est $O(x^2 + 2x + 1)$, car $x^2 < x^2 + 2x + 1$ chaque fois que $x > 1$. Ce signifie que $C = 1$ et $k = 1$ sont témoins de la relation x^2 est $O(x^2 + 2x + 1)$. ▲

Notez que dans l'exemple 1, nous avons deux fonctions, $f(x) = x^2 + 2x + 1$ et $g(x) = x^2$, telles que $f(x)$ est $O(g(x))$ et $g(x)$ est $O(f(x))$ - ce dernier fait résultant de l'inégalité $x^2 \leq x^2 + 2x + 1$, qui vaut pour tous les nombres réels non négatifs x . Nous disons que deux fonctions Les relations $f(x)$ et $g(x)$ qui satisfont ces deux grandes relations O sont du **même ordre** . nous reviendra sur cette notion plus loin dans cette section.

Remarque: Le fait que $f(x)$ soit $O(g(x))$ s'écrit parfois $f(x) = O(g(x))$. Cependant, le signe égal dans cette notation ne représente *pas* une véritable égalité. Au contraire, cette notation indique nous savons qu'une inégalité existe concernant les valeurs des fonctions f et g pour des valeurs suffisamment dans les domaines de ces fonctions. Cependant, il est acceptable d'écrire $f(x) \in O(g(x))$ parce que $O(g(x))$ représente l'ensemble des fonctions qui sont $O(g(x))$.

Lorsque $f(x)$ est $O(g(x))$, et $h(x)$ est une fonction qui a de plus grandes valeurs absolues que $g(x)$ fait pour des valeurs suffisamment grandes de x , il s'ensuit que $f(x)$ est $O(h(x))$. En d'autres termes, la fonction $g(x)$ dans la relation $f(x)$ est $O(g(x))$ peut être remplacé par une fonction avec un plus grand absolu valeurs. Pour voir cela, notez que si

$$|f(x)| \leq C|g(x)| \qquad \text{si } x > k,$$

et si $|h(x)| > |g(x)|$ pour tout $x > k$, alors

$$|f(x)| \leq C|h(x)| \qquad \text{si } x > k.$$

Par conséquent, $f(x)$ est $O(h(x))$.

Lorsque la notation big- O est utilisée, la fonction g dans la relation $f(x)$ est $O(g(x))$ est choisie être aussi petit que possible (parfois à partir d'un ensemble de fonctions de référence, telles que les fonctions forme x^n , où n est un entier positif).

PAUL GUSTAV HEINRICH BACHMANN (1837–1920) Paul Bachmann, fils d'un pasteur luthérien, a partagé le style de vie pieux et l'amour de la musique de son père. Son talent mathématique a été découvert par l'un de ses professeurs, même bien qu'il ait eu des difficultés avec certaines de ses premières études mathématiques. Après avoir récupéré de la tuberculose en Suisse, Bachmann a étudié les mathématiques, d'abord à l'Université de Berlin puis à Göttingen, où il a assisté à des conférences présentées par le célèbre théoricien des nombres Dirichlet. Il a obtenu son doctorat sous la Théoricien allemand des nombres Kummer en 1862; sa thèse portait sur la théorie des groupes. Bachmann était professeur à Breslau et plus tard à Münster. Après sa retraite de sa chaire, il a continué son écriture mathématique, joué le piano, et a été critique musical pour les journaux. Les écrits mathématiques de Bachmann comprennent cinq volumes enquête sur les résultats et les méthodes de la théorie des nombres, un ouvrage en deux volumes sur la théorie élémentaire des nombres, un livre sur des nombres irrationnels et un livre sur la fameuse conjecture connue sous le nom de Dernier Théorème de Fermat. Il a introduit la notation big- O dans son 1892 livre *Analytische Zahlentheorie.*

EDMUND LANDAU (1877–1938) Edmund Landau, fils d'un gynécologue berlinois, fréquenta l'école secondaire et l'université de Berlin. Il obtient son doctorat en 1899, sous la direction de Frobenius. Landau a d'abord enseigné à l'Université de Berlin, puis a déménagé à Göttingen, où il a été professeur ordinaire jusqu'à ce que les nazis ont forcé lui d'arrêter d'enseigner. Landau a principalement contribué aux mathématiques dans le domaine de la théorie analytique des nombres. En particulier, il a établi plusieurs résultats importants concernant la distribution des nombres premiers. Il est l'auteur d'un exposition en trois volumes sur la théorie des nombres ainsi que d'autres livres sur la théorie des nombres et l'analyse mathématique.

Cg (*x*)

f (*x*)

La partie du graphique de *f* (*x*) qui satisfait
f (*x*) < *Cg* (*x*) est affiché en couleur.

g (*x*)

f (*x*) < *Cg* (*x*) pour *x* > *k*

k

FIGURE 2 La fonction $f(x)$ **est** $O(g(x))$ **.**

Dans les discussions ultérieures, nous traiterons presque toujours des fonctions qui valeurs positives. Toutes les références aux valeurs absolues peuvent être supprimées lorsque vous travaillez avec big-O estimations pour ces fonctions. La figure 2 illustre la relation $f(x)$ est $O(g(x))$.

L'exemple 2 illustre comment la notation big- O est utilisée pour estimer la croissance des fonctions.

EXEMPLE 2 Montrez que $7x^2$ est $O(x^3)$.

Solution: Notez que lorsque $x > 7$, nous avons $7x^2 < x^3$. (On peut obtenir cette inégalité en multipliant les deux côtés de $x > 7$ par x^2.) Par conséquent, nous pouvons prendre $C = 1$ et $k = 7$ comme témoins pour établir

DONALD E. KNUTH (NÉ EN 1938) Knuth a grandi à Milwaukee, où son père a enseigné la comptabilité à un lycée luthérien et possédait une petite entreprise d'impression. Il était un excellent étudiant, gagnant des études prix de réussite. Il a appliqué son intelligence de manière non conventionnelle, remportant un concours lorsqu'il était huitième année en trouvant plus de 4500 mots qui pourraient être formés à partir des lettres dans "Ziegler's Giant Bar". Cette a remporté un poste de télévision pour son école et un bar à bonbons pour tout le monde dans sa classe.

Knuth a eu du mal à choisir la physique plutôt que la musique comme son principal au Case Institute of Technology. Il puis passe de la physique aux mathématiques et, en 1960, il obtient son baccalauréat ès sciences, simultanément recevant une maîtrise ès sciences par un prix spécial de la faculté qui considérait son travail comme exceptionnel. Chez Case, il a dirigé l'équipe de basket-ball et a appliqué ses talents en construisant une formule pour la valeur de chaque joueur. Cette nouvelle approche a été couverte par *Newsweek* et par Walter Cronkite sur le réseau de télévision CBS. Knuth a commencé ses études travailler au California Institute of Technology en 1960 et a obtenu son doctorat. là en 1963. Pendant ce temps, il a travaillé comme consultant, écrire des compilateurs pour différents ordinateurs.

Knuth a rejoint le personnel du California Institute of Technology en 1963, où il est resté jusqu'en 1968, date à laquelle il a accepté un poste de professeur titulaire à l'Université de Stanford. Il a pris sa retraite en tant que professeur émérite en 1992 pour se concentrer sur l'écriture. Il est particulièrement intéressé dans la mise à jour et l'achèvement de nouveaux volumes de sa série *The Art of Computer Programming,* une œuvre qui a eu une profonde influence sur le développement de l'informatique, qu'il a commencé à écrire en tant qu'étudiant diplômé en 1962, en se concentrant sur les compilateurs. En commun jargon, "Knuth", se référant à *l'Art de la programmation informatique,* est devenu la référence qui répond à toutes les questions sur des sujets tels que les structures de données et les algorithmes.

Knuth est le fondateur de l'étude moderne de la complexité informatique. Il a apporté des contributions fondamentales au sujet de compilateurs. Son mécontentement à l'égard de la typographie mathématique l'a incité à inventer les systèmes TeX et Metafont maintenant largement utilisés. TeX est devenu un langage standard pour la typographie informatique. Deux des nombreux prix que Knuth a reçus sont les Turing de 1974 Prix et la Médaille nationale de technologie de 1979, décernée par le président Carter.

Knuth a écrit pour un large éventail de revues professionnelles en informatique et en mathématiques. Cependant, sa première publication, en 1957, quand il était étudiant de première année, était une parodie du système métrique appelé "Les systèmes de poids de Potrzebie and Measures », paru dans *MAD Magazine* et réimprimé à plusieurs reprises. Il est organiste d'église, comme l'était son père. Il est également compositeur de musique pour orgue. Knuth croit que l'écriture de programmes informatiques peut être une expérience esthétique, beaucoup comme écrire de la poésie ou composer de la musique.

Knuth paie 2,56 $ pour la première personne à trouver chaque erreur dans ses livres et 0,32 $ pour des suggestions importantes. Si vous lui envoyez une lettre avec une erreur (vous devrez utiliser le courrier normal, car il a abandonné la lecture des e-mails), il vous informera éventuellement si vous avez été la première personne à lui signaler cette erreur. Soyez prêt pour une longue attente, car il reçoit une écrasante quantité de courrier. (L'auteur a reçu une lettre des années après avoir envoyé un rapport d'erreur à Knuth, notant que ce rapport est arrivé plusieurs fois mois après le premier signalement de cette erreur.)

la relation $7x^2$ est $O(x^3)$. Alternativement, lorsque $x > 1$, nous avons $7x^2 < 7x^3$, de sorte que $C = 7$ et $k = 1$ sont également témoins de la relation $7x^2$ est $O(x^3)$. ▲

L'exemple 3 montre comment montrer qu'une relation big- O ne tient pas.

EXEMPLE 3 Montrer que n^2 n'est pas $O(n)$.

Solution: Pour montrer que n^2 est pas $O(n)$, nous devons montrer qu'aucune paire de témoins C et k exist tel que $n^2 \leq Cn$ chaque fois que $n > k$. Nous utiliserons une preuve par contradiction pour le montrer.

Supposons qu'il existe des constantes C et k pour lesquelles $n^2 \leq Cn$ chaque fois que $n > k$. Observe ceci lorsque $n > 0$, nous pouvons diviser les deux côtés de l'inégalité $n^2 \leq Cn$ par n pour obtenir l'équivalent inégalité $n \leq C$. Cependant, peu importe ce que sont C et k, l'inégalité $n \leq C$ ne peut pas tenir pour tous n avec $n > k$. En particulier, une fois que nous avons défini une valeur de k, nous voyons que lorsque n est plus grand que le maximum de k et C, il n'est pas vrai que $n \leq C$ même si $n > k$. Cette contradiction montre que n^2 dans pas $O(n)$. ▲

EXEMPLE 4 L' exemple 2 montre que $7x^2$ est $O(x^3)$. Est-il également vrai que x^3 est $O(7x^2)$?

Solution: Pour déterminer si x^3 est $O(7x^2)$, nous devons déterminer si les témoins C et k existe, de sorte que $x^3 \leq C(7x^2)$ chaque fois que $x > k$. Nous montrerons qu'il n'existe pas de tels témoins une preuve par contradiction.

Si C et k sont témoins, l'inégalité $x^3 \leq C(7x^2)$ est valable pour tout $x > k$. Observez que le l'inégalité $x^3 \leq C(7x^2)$ est équivalente à l'inégalité $x \leq 7C$, qui suit en divisant les deux côtés par la quantité positive x^2. Cependant, quel que soit C, il n'est pas vrai que $x \leq 7C$ pour tout $x > k$ quel que soit k, car x peut être arbitrairement grand. Il s'ensuit qu'aucun les témoins C et k existent pour cette relation big- O proposée. Par conséquent, x^3 n'est *pas* $O(7x^2)$. ▲

Estimations Big- *O* pour certaines fonctions importantes

Les polynômes peuvent souvent être utilisés pour estimer la croissance des fonctions.Au lieu d'analyser la croissance des polynômes à chaque fois qu'ils se produisent, nous aimerions un résultat qui puisse toujours être utilisé estimer la croissance d'un polynôme. Le théorème 1 fait cela. Il montre que le terme principal d'un le polynôme domine sa croissance en affirmant qu'un polynôme de degré n ou moins est $O(x^n)$.

THÉORÈME 1 Soit $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, où $a_0, a_1, \ldots, a_{n-1}, a_n$ sont nombre réel bers. Alors $f(x)$ est $O(x^n)$.

Preuve: en utilisant l'inégalité du triangle (voir exercice 7 dans la section 1.8), si $x > 1$ nous avons

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0| \\ &\leq |a_n| x^n + |a_{n-1}| x^{n-1} + \cdots + |un_1| x + |un_0| \\ &= x^n \left(|a_n| + |a_{n-1}| / x + \cdots + |un_1| / x^{n-1} + |un_0| / x^n \right) \\ &\leq x^n (|a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|). \end{aligned}$$

Cela montre que

$$|f(x)| \leq Cx^n,$$

où $C = |a_n| + |a_{n-1}| + \cdots + |a_0|$ chaque fois que $x > 1$. Par conséquent, les témoins $C = |a_n| + |a_{n-1}| + \cdots + |un_0|$ et $k = 1$ montrent que $f(x)$ est $O(x^n)$.

Nous donnons maintenant quelques exemples impliquant des fonctions qui ont l'ensemble d'entiers positifs comme leurs domaines.

EXEMPLE 5 Comment utiliser la notation big- O pour estimer la somme des n premiers entiers positifs?

Solution: Parce que chacun des entiers dans la somme des n premiers entiers positifs ne dépasse pas n, il s'ensuit que

$$1 + 2 + \cdots + n \leq n + n + \cdots + n = n^2.$$

De cette inégalité, il s'ensuit que $1 + 2 + 3 + \cdots + n$ est $O(n^2)$, en prenant $C = 1$ et $k = 1$ comme les témoins. (Dans cet exemple, les domaines des fonctions dans la relation big- O sont l'ensemble des entiers positifs.) ▲

Dans l'exemple 6, des estimations du grand O seront développées pour la fonction factorielle et sa logarithm. Ces estimations seront importantes dans l'analyse du nombre d'étapes utilisées dans le tri procédures.

EXEMPLE 6 Donner des estimations de grand O pour la fonction factorielle et le logarithme de la fonction factorielle, où la fonction factorielle $f(n) = n!$ est défini par

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$$

chaque fois que n est un entier positif, et $0! = 1$. Par exemple,

$$1! = 1,\ 2! = 1 \cdot 2 = 2,\ 3! = 1 \cdot 2 \cdot 3 = 6,\ 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24.$$

Notez que la fonction $n!$ croît rapidement. Par exemple,

$$20! = 2,432,902,008,176,640,000.$$

Solution: une estimation big- O pour $n!$ peut être obtenu en notant que chaque terme du produit ne ne pas dépasser n. Par conséquent,

$$\begin{aligned} n! &= 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n \\ &\leq n \cdot n \cdot n \cdot \cdots \cdot n \\ &= n^n. \end{aligned}$$

Cette inégalité montre que $n!$ est $O(n^n)$, en prenant $C = 1$ et $k = 1$ comme témoins. Prendre des logarithmes des deux côtés de l'inégalité établie pour $n!$, on obtient

$$\log n! \leq \log n^n = n \log n.$$

Cela implique que $\log n!$ est $O(n \log n)$, prenant encore $C = 1$ et $k = 1$ comme témoins. ▲

EXEMPLE 7 Dans la section 4.1, nous montrerons que $n < 2^n$ chaque fois que n est un entier positif. Montrez que cela l'inégalité implique que n est $O(2^n)$, et utilisez cette inégalité pour montrer que $\log n$ est $O(n)$.

Solution: en utilisant l'inégalité $n < 2^n$, nous pouvons rapidement conclure que n est $O(2^n)$ en prenant $k = C = 1$ comme témoins. Notez que parce que la fonction logarithme augmente, en prenant des logarithmes (base 2) des deux côtés de cette inégalité montre que

$$\log n < n.$$

Il s'ensuit que

$$\log n \text{ est } O(n).$$

(Encore une fois, nous prenons $C = k = 1$ comme témoins.)

Si nous avons des logarithmes à une base b, où b est différent de 2, nous avons toujours $\log_b n$ est $O(n)$ car

$$\log_b n = \frac{\log n}{\log b} < \frac{n}{\log b}$$

chaque fois que n est un entier positif. Nous prenons $C = 1 / \log b$ et $k = 1$ comme témoins. (Nous avons utilisé Théorème 3 en annexe 2 pour voir que $\log_b n = \log n / \log b$.) ▲

Comme mentionné précédemment, la notation big- O est utilisée pour estimer le nombre d'opérations résoudre un problème à l'aide d'une procédure ou d'un algorithme spécifié. Les fonctions utilisées dans ces estimations comprennent souvent les éléments suivants:

$$1,\ \log n,\ n,\ n \log n,\ n^2,\ 2^n,\ n!$$

En utilisant le calcul, on peut montrer que chaque fonction de la liste est plus petite que la suivante fonction, dans le sens où le rapport d'une fonction et de la fonction suivante tend vers zéro comme n grandit sans limite. La figure 3 affiche les graphiques de ces fonctions, en utilisant une échelle pour les valeurs des fonctions qui doublent pour chaque marquage successif sur le graphe.C'est le l'échelle verticale dans ce graphique est logarithmique.

$n!$

4096
2048
1024
512
256
128
64
32
16
8
4
2
1

2^n — n^2 — $n \log n$ — n — $\log n$ — 1

2 3 4 5 6 sept 8

FIGURE 3 **Un affichage de la croissance des fonctions couramment utilisées dans les estimations Big-** ***O*** **.**

BIG- ***O*** **ESTIMATIONS UTILES IMPLIQUANT LES LOGARITHMES, LES POUVOIRS ET LES FONCTIONS TIALES** Nous donnons maintenant quelques faits utiles qui nous aident à déterminer si gros-O relations entre paires de fonctions lorsque chacune des fonctions est une puissance de logarithme, une puissance ou une fonction exponentielle de la forme b^n où $b > 1$. Leurs preuves restent comme Exercices 57 à 60 pour les lecteurs expérimentés en calcul.

Le théorème 1 montre que si $f(n)$ est un polynôme de degré d, alors $f(n)$ est $O(n^d)$. Appliquer ce théorème, nous voyons que si $d > c > 1$, alors n^c est $O(n^d)$. Nous laissons au lecteur le soin de montrer que l'inverse de cette relation ne tient pas. En rassemblant ces faits, nous voyons que si $d > c > 1$, puis

$$n^c \text{ est } O(n^d), \text{ mais } n^d \text{ n'est pas } O(n^c).$$

Dans l'exemple 7, nous avons montré que $\log_b n$ est $O(n)$ chaque fois que $b > 1$. Plus généralement, chaque fois que $b > 1$ et c et d sont positifs, nous avons

$$(\log_b n)^c \text{ est } O(n^d), \text{ mais } n^d \text{ n'est pas } (O(\log_b n)^c).$$

Cela nous dit que chaque puissance positive du logarithme de n à la base b, où $b > 1$, est grande -O de chaque puissance positive de n, mais la relation inverse ne tient jamais.

Dans l'exemple 7, nous avons également montré que n est $O(2^n)$. Plus généralement, chaque fois que d est positif et $b > 1$, nous avons

$$n^d \text{ est } O(b^n), \text{ mais } b^n \text{ n'est pas } O(n^d).$$

Cela nous dit que chaque puissance de n est grande -O de chaque fonction exponentielle de n avec une base qui est supérieur à un, mais la relation inverse ne tient jamais. De plus, nous avons quand $c > b > 1$,

$$b^n \text{ est } O(c^n) \text{ mais } c^n \text{ n'est pas } O(b^n).$$

Cela nous dit que si nous avons deux fonctions exponentielles avec des bases différentes supérieures à une, une de ces fonctions est grand -O de l'autre si et seulement si sa base est plus petite ou égale.

La croissance des combinaisons de fonctions

De nombreux algorithmes sont constitués de deux sous-procédures distinctes ou plus. Le nombre d'étapes utilisé par un ordinateur pour résoudre un problème avec une entrée d'une taille spécifiée en utilisant un tel algorithme est la somme du nombre d'étapes utilisées par ces sous-procédures. Pour donner une estimation de grand O pour la nombre d'étapes nécessaires, il est nécessaire de trouver des estimations de grand O pour le nombre d'étapes utilisées par chaque sous-procédure, puis combiner ces estimations.

Des estimations Big- O des combinaisons de fonctions peuvent être fournies si des précautions sont prises lorsque différentes *Les* estimations bigO sont combinées. En particulier, il est souvent nécessaire d'estimer la croissance de la somme et le produit de deux fonctions. Que peut-on dire si big- O estime pour chacun des deux les fonctions sont connues? Pour voir quel genre d'estimations détiennent la somme et le produit de deux fonctions, supposons que $f_1(x)$ est $O(g_1(x))$ et $f_2(x)$ est $O(g_2(x))$.

D'après la définition de la notation big- O, il existe des constantes C_1, C_2, k_1 et k_2 telles que

$$|f_1(x)| \le C_1 |g_1(x)|$$

lorsque $x > k_1$, et

$$|f_2(x)| \leq C_2 |g_2(x)|$$

lorsque $x > k_2$. Pour estimer la somme de $f_1(x)$ et $f_2(x)$, notez que

$$\begin{aligned} |(f_1 + f_2)(x)| &= |f_1(x) + f_2(x)| \\ &\leq |f_1(x)| + |f_2(x)| \quad \text{en utilisant l'inégalité du triangle } |a+b| \leq |a| + |b| . \end{aligned}$$

Lorsque x est supérieur à la fois à k_1 et à k_2 , il résulte des inégalités pour $|f_1(x)|$ et $|f_2(x)|$ cette

$$\begin{aligned} |f_1(x)| + |f_2(x)| &\leq C_1 |g_1(x)| + C_2 |g_2(x)| \\ &\leq C_1 |g(x)| + C_2 |g(x)| \\ &= (C_1 + C_2) |g(x)| \\ &= C |g(x)| , \end{aligned}$$

où $C = C_1 + C_2$ et $g(x) = \max(|g_1(x)|, |g_2(x)|)$. [Ici max (a, b) désigne le maximum, ou plus, de a et b .]

Cette inégalité montre que $|(f_1 + f_2)(x)| \leq C |g(x)|$ chaque fois que $x > k$, où $k = \max(k_1, k_2)$. Nous déclarons ce résultat utile comme Théorème 2.

THÉORÈME 2 Supposons que $f_1(x)$ soit $O(g_1(x))$ et que $f_2(x)$ soit $O(g_2(x))$. Alors $(f_1 + f_2)(x)$ est $O(\max(|g_1(x)|, |g_2(x)|))$.

Nous avons souvent des estimations de grand O pour f_1 et f_2 en fonction de la même fonction g . Dans cette situation, Le théorème 2 peut être utilisé pour montrer que $(f_1 + f_2)(x)$ est également $O(g(x))$, car $\max(g(x), g(x)) = g(x)$. Ce résultat est indiqué dans le corollaire 1.

COROLLARY 1 Supposons que $f_1(x)$ et $f_2(x)$ soient tous les deux $O(g(x))$. Alors $(f_1 + f_2)(x)$ est $O(g(x))$.

De la même manière, des estimations du grand O peuvent être dérivées pour le produit des fonctions f_1 et f_2 . Lorsque x est supérieur à $\max(k_1, k_2)$, il s'ensuit que

$$\begin{aligned} |(f_1 f_2)(x)| &= |f_1(x)||f_2(x)| \\ &\leq C_1 |g_1(x)| C_2 |g_2(x)| \\ &\leq C_1 C_2 |(g_1 g_2)(x)| \\ &\leq C |(g_1 g_2)(x)| , \end{aligned}$$

où $C = C_1 C_2$. De cette inégalité, il s'ensuit que $f_1(x) f_2(x)$ est $O(g_1 g_2(x))$, car il existe des constantes C et k , à savoir $C = C_1 C_2$ et $k = \max(k_1, k_2)$, telles que $|(f_1 f_2)(x)| \leq C |g_1(x) g_2(x)|$ chaque fois que $x > k$. Ce résultat est énoncé dans le théorème 3.

THÉORÈME 3 Supposons que $f_1(x)$ est $O(g_1(x))$ et $f_2(x)$ est $O(g_2(x))$. Alors $(f_1 f_2)(x)$ est $O(g_1(x) g_2(x))$.

Le but en utilisant la notation big- O pour estimer des fonctions est de choisir une fonction $g(x)$ aussi simple que possible, cela croît relativement lentement de sorte que $f(x)$ est $O(g(x))$. Les exemples 8 et 9 illustrent comment utiliser les théorèmes 2 et 3 pour ce faire.Le type d'analyse donné dans ces exemples est souvent utilisé dans l'analyse du temps utilisé pour résoudre les problèmes à l'aide de programmes informatiques.

EXEMPLE 8 Donner une estimation big- O pour $f(n) = 3n \log(n!) + (N^2 + 3) \log n$, où n est un entier positif.

Solution: Tout d'abord, le produit $3n \log(n!)$ Sera estimé. De l'exemple 6, nous savons que $\log(n!)$ est $O(n \log n)$. En utilisant cette estimation et le fait que $3n$ est $O(n)$, le théorème 3 donne l'estimation que $3n \log(n!)$ est $O(n^2 \log n)$.

Ensuite, le produit $(n^2 + 3) \log n$ sera estimé. Parce que $(n^2 + 3) < 2n^2$ lorsque $n > 2$, il s'ensuit que $n^2 + 3$ est $O(n^2)$. Ainsi, du théorème 3, il s'ensuit que $(n^2 + 3) \log n$ est $O(n^2 \log n)$. L'utilisation du théorème 2 pour combiner les deuxestimations de grand O pour les produits montre que $f(n) = 3n \log(n!) + (N^2 + 3) \log n$ est $O(n^2 \log n)$. ▲

EXEMPLE 9 Donner une estimation big- O pour $f(x) = (x + 1) \log(x^2 + 1) + 3x^2$.

Solution: Tout d'abord, une estimation big- O pour $(x + 1) \log(x^2 + 1)$ sera trouvée. Notez que $(x + 1)$ est $O(x)$. De plus, $x^2 + 1 \leq 2x^2$ lorsque $x > 1$. Par conséquent,

$$\log(x^2 + 1) \leq \log(2x^2) = \log 2 + \log x^2 = \log 2 + 2 \log x \leq 3 \log x,$$

si $x > 2$. Cela montre que $\log(x^2 + 1)$ est $O(\log x)$.

Du Théorème 3, il s'ensuit que $(x + 1) \log(x^2 + 1)$ est $O(x \log x)$. Parce que $3x^2$ est $O(x^2)$, Le théorème 2 nous dit que $f(x)$ est $O(\max(x \log x, x^2))$. Parce que $x \log x \leq x^2$, pour $x > 1$, il suit que $f(x)$ est $O(x^2)$. ▲

Notation Big-Omega et Big-Theta

et sont les grecs lettres majuscules oméga et thêta, respectivement.

La notation Big- O est largement utilisée pour décrire la croissance des fonctions, mais elle a ses limites. Dans en particulier, lorsque $f(x)$ est $O(g(x))$, nous avons une limite supérieure, en termes de $g(x)$, pour la taille de $f(x)$ pour les grandes valeurs de x. Cependant, la notation big- O ne fournit pas de limite inférieure pour la taille de $f(x)$ pour grand x. Pour cela, nous utilisons la **notation big-Omega (big-)**. Quand on veut donner à la fois une et une borne inférieure sur la taille d'une fonction $f(x)$, par rapport à une fonction de référence $g(x)$, nous utilisons **big-Notation thêta (grande)**. La notation big-Omega et big-Theta a été introduite par Donald Knuth dans les années 1970. Sa motivation pour introduire ces notations était l'utilisation abusive notation big- O quand une borne supérieure et une borne inférieure de la taille d'une fonction sont nécessaires.

Nous définissons maintenant la notation big-Omega et illustrons son utilisation. Après cela, nous ferons le idem pour la notation big-Theta.

DÉFINITION 2 Soit f et g *des* fonctions de l'ensemble des entiers ou de l'ensemble des nombres réels à l'ensemble des réels Nombres. On dit que $f(x)$ est $(g(x))$ s'il y a des constantes positives C et k telles que

$$|f(x)| \geq C|g(x)|$$

chaque fois que $x > k$. [Ceci est lu comme « $f(x)$ est un grand oméga de $g(x)$.»]

Il existe une forte connexion entre la notation big- O et big-Omega. En particulier, $f(x)$ est $(g(x))$ si et seulement si $g(x)$ est $O(f(x))$. Nous laissons la vérification de ce fait simple exercice pour le lecteur.

EXEMPLE 10 La fonction $f(x) = 8x^3 + 5x^2 + 7$ est $(g(x))$, où $g(x)$ est la fonction $g(x) = x^3$. Cette est facile à voir car $f(x) = 8x^3 + 5x^2 + 7 \geq 8x^3$ pour tous les nombres réels positifs x. C'est équivaut à dire que $g(x) = x^3$ est $O(8x^3 + 5x^2 + 7)$, qui peut être établi directement par renverser l'inégalité. ▲

Souvent, il est important de connaître l'ordre de croissance d'une fonction en termes de fonction de référence simple telle que x^n lorsque n est un entier positif ou c^x, où $c > 1$. Connaître l'ordre de croissance exige que nous ayons à la fois une limite supérieure et une limite inférieure pour la taille de la fonction. Autrement dit, étant donné une fonction $f(x)$, nous voulons une fonction de référence $g(x)$ telle que $f(x)$ est $O(g(x))$ et $f(x)$ est $(g(x))$. La notation Big-Theta, définie comme suit, est utilisée pour exprimer à la fois de ces relations, fournissant à la fois une limite supérieure et une limite inférieure sur la taille d'une fonction.

DÉFINITION 3 Soit f et g *des* fonctions de l'ensemble des entiers ou de l'ensemble des nombres réels à l'ensemble des réels Nombres. Nous disons que $f(x)$ est $(g(x))$ si $f(x)$ est $O(g(x))$ et $f(x)$ est $(g(x))$. Lorsque $f(x)$ est $(g(x))$ on dit que f est grand-Thêta de $g(x)$, que $f(x)$ est d' *ordre* $g(x)$, et que $f(x)$ et $g(x)$ sont du *même ordre* .

Lorsque $f(x)$ est $(g(x))$, il est également vrai que $g(x)$ est $(f(x))$. Notez également que $f(x)$ est $(g(x))$ si et seulement si $f(x)$ est $O(g(x))$ et $g(x)$ est $O(f(x))$ (voir exercice 31). De plus, notez que $f(x)$ est $(g(x))$ si et seulement s'il y a des nombres réels C_1 et C_2 et un nombre réel positif k tel que

$$C_1 |g(x)| \leq |f(x)| \leq C_2 |g(x)|$$

chaque fois que $x > k$. L'existence des constantes C_1, C_2 et k nous indique que $f(x)$ est $(g(x))$ et que $f(x)$ est $O(g(x))$, respectivement.

Habituellement, lorsque la notation big-Theta est utilisée, la fonction $g(x)$ dans $(g(x))$ est relativement simple fonction de référence, telle que x^n, c^x, $\log x$, etc., tandis que $f(x)$ peut être relativement compliqué.

EXEMPLE 11 Nous avons montré (dans l'exemple 5) que la somme des n premiers entiers positifs est $O(n^2)$. Est-ce que cette somme de ordre n^2 ?

Solution: Soit $f(n) = 1 + 2 + 3 + \cdots + n$. Parce que nous savons déjà que $f(n)$ est $O(n^2)$, montrer que $f(n)$ est d'ordre n^2 nous devons trouver une constante positive C telle que $f(n) > Cn^2$ pour entiers suffisamment grands n. Pour obtenir une borne inférieure pour cette somme, nous pouvons ignorer la première moitié des termes. En sommant uniquement les termes supérieurs à $\lceil n/2 \rceil$, nous constatons que

$$\begin{aligned}
1 + 2 + \cdots + n &\geq \lceil n/2 \rceil + (\lceil n/2 \rceil + 1) + \cdots + n \\
&\geq \lceil n/2 \rceil + \lceil n/2 \rceil + \cdots + \lceil n/2 \rceil \\
&= (n - \lceil n/2 \rceil + 1) \lceil n/2 \rceil \\
&\geq (n/2)(n/2) \\
&= N_{\text{deux}}/4 .
\end{aligned}$$

Cela montre que $f(n)$ est (n^2). Nous concluons que $f(n)$ est d'ordre n^2, ou en symboles, $f(n)$ est (n^2). ▲

EXEMPLE 12 Montrer que $3x^2 + 8x \log x$ est (x^2).

Solution: Parce que $0 \leq 8x \log x \leq 8x^2$, il s'ensuit que $3x^2 + 8x \log x \leq 11x^2$ pour $x > 1$. Par conséquent, $3x^2 + 8x \log x$ est $O(x^2)$. Clairement, x^2 est $O(3x^2 + 8x \log x)$. Par conséquent, $3x^2 + 8x \log x$ est (x^2). ▲

Un fait utile est que le terme principal d'un polynôme détermine son ordre. Par exemple, si $f(x) = 3x^5 + x^4 + 17x^3 + 2$, alors $f(x)$ est d'ordre x^5. Ceci est indiqué dans le théorème 4, dont la preuve est laissée comme exercice 50.

THÉORÈME 4 Soit $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, où $a_0, a_1, \ldots, a_n$ sont des nombres réels avec $a_n = 0$. Alors $f(x)$ est d'ordre x^n.

EXEMPLE 13 Les polynômes $3x^8 + 10x^7 + 221x^2 + 1444$, $x^{19} - 18x^4 - 10{,}112$ et $-x^{99} + 40{,}001x^{98} + 100{,}003x$ sont d'ordres x^8, x^{19} et x^{99}, respectivement. ▲

Malheureusement, comme l'a observé Knuth, la notation big- O est souvent utilisée par haut-parleurs comme si elle avait la même signification que la notation big-Theta. Gardez cela à l'esprit lorsque vous voyez big- notation O utilisée. La tendance récente a été d'utiliser la notation big-thêta chaque fois que et des limites inférieures sur la taille d'une fonction sont nécessaires.

Des exercices

Dans les exercices 1 à 14, pour établir une grande relation O, trouvez nesses C et k telles que $|f(x)| \leq C|g(x)|$ chaque fois que $x > k$.

1. Déterminez si chacune de ces fonctions est $O(x)$.

a) $f(x) = 10$ **b)** $f(x) = 3x + 7$
c) $f(x) = x^2 + x + 1$ **d)** $f(x) = 5 \log x$
e) $f(x) = \lfloor x \rfloor$ **f)** $f(x) = \lceil x/2 \rceil$

2. Déterminez si chacune de ces fonctions est $O(x^2)$.

a) $f(x) = 17x + 11$ **b)** $f(x) = x^2 + 1000$
c) $f(x) = x \log x$ **d)** $f(x) = x^4/$deux
e) $f(x) = 2^x$ **f)** $f(x) = \lfloor x \rfloor \cdot \lceil x \rceil$

3. Utilisez la définition de « $f(x)$ est $O(g(x))$ » pour montrer que $x^4 + 9x^3 + 4x + 7$ est $O(x^4)$.

4. Utilisez la définition de « $f(x)$ est $O(g(x))$ » pour montrer que $2^x + 17$ est $O(3^x)$.

5. Montrez que $(x^2 + 1)/(x + 1)$ est $O(x)$.

6. Montrez que $(x^3 + 2x)/(2x + 1)$ est $O(x^2)$.

7. Trouvez le plus petit entier n tel que $f(x)$ soit $O(x^n)$ pour chaque de ces fonctions.

a) $f(x) = 2x^3 + x^2 \log x$
b) $f(x) = 3x^3 + (\log x)^4$
c) $f(x) = (x^4 + x^2 + 1)/(x^3 + 1)$
d) $f(x) = (x^4 + 5 \log x)/(x^4 + 1)$

8. Trouvez le plus petit entier n tel que $f(x)$ soit $O(x^n)$ pour chaque de ces fonctions.

a) $f(x) = 2x^2 + x^3 \log x$
b) $f(x) = 3x^5 + (\log x)^4$
c) $f(x) = (x^4 + x^2 + 1)/(x^4 + 1)$
d) $f(x) = (x^3 + 5 \log x)/(x^4 + 1)$

9. Montrez que $x^2 + 4x + 17$ est $O(x^3)$ mais que x^3 n'est pas $O(x^2 + 4x + 17)$.

10. Montrez que x^3 est $O(x^4)$ mais que x^4 n'est pas $O(x^3)$.

11. Montrer que $3x^4 + 1$ est $O(x^4/2)$ et $x^4/2$ est $O(3x^4 + 1)$.

12. Montrez que $x \log x$ est $O(x^2)$ mais que x^2 n'est pas $O(x \log x)$.

13. Montrez que 2^n est $O(3^n)$ mais que 3^n n'est pas $O(2^n)$. (Notez que il s'agit d'un cas particulier de l'exercice 60.)

14. Déterminez si x^3 est $O(g(x))$ pour chacune de ces fonctions. tions $g(x)$.

a) $g(x) = x^2$ **b)** $g(x) = x^3$
c) $g(x) = x^2 + x^3$ **d)** $g(x) = x^2 + x^4$
e) $g(x) = 3^x$ **f)** $g(x) = x^3/$deux

15. Expliquez ce que signifie qu'une fonction est $O(1)$.

16. Montrez que si $f(x)$ est $O(x)$, alors $f(x)$ est $O(x^2)$.

17. Supposons que $f(x)$, $g(x)$ et $h(x)$ sont des fonctions telles que $f(x)$ est $O(g(x))$ et $g(x)$ est $O(h(x))$. Montrer que $f(x)$ est $O(h(x))$.

18. Soit k un entier positif. Montrez que $1^k + 2^k + \cdots + n^k$ est $O(n^{k+1})$.

19. Déterminez si chacune des fonctions 2^{n+1} et 2^{2n} est $O(2^n)$.

20. Déterminez si chacune des fonctions $\log(n + 1)$ et $\log(n^2 + 1)$ est $O(\log n)$.

21. Organiser les fonctions $\sqrt{n}$, $1000 \log n$, $n \log n$, $2n!$, 2^n, 3^n, et $n^2/1{,}000{,}000$ dans une liste de telle sorte que chaque fonction est Big - O de la fonction suivante.

22. Disposer la fonction $(1.5)^n$, n^{100}, $(\log n)^3$, $\sqrt{n} \log n$, 10^n, $(n!)^2$, et $n^{99} + n^{98}$ dans une liste pour que chaque fonction soit grande - O de la fonction suivante.

23. Supposons que vous ayez deux algorithmes différents pour un problème. Pour résoudre un problème de taille n, le premier algorithme utilise exactement $n(\log n)$ opérations et la sec- ond algorithme utilise exactement $n^{3/2}$ opérations. Au fur et à mesure que n grandit, quel algorithme utilise moins d'opérations?

24. Supposons que vous ayez deux algorithmes différents pour un problème. Pour résoudre un problème de taille n, le premier l'algorithme utilise exactement $n^2 2^n$ opérations et la seconde l'algorithme utilise exactement $n!$ opérations. Au fur et à mesure que n grandit, algorithme utilise moins d'opérations?

25. Donner aussi bon Big- O estimation possible pour chacun des ces fonctions.

a) $(n^2 + 8)(n + 1)$ **b)** $(n \log n + n^2)(n^3 + 2)$
c) $(n! + 2^n)(n^3 + \log(n^2 + 1))$

39. Montrer que si f et g sont des fonctions à valeur réelle telles que $f(x)$ est $O(g(x))$, alors pour chaque entier positif n, $f^n(x)$ est $O(g^n(x))$. [Notez que $f^n(x) = f(x)^n$.]

40. Montrez que pour tous les nombres réels a et b avec $a > 1$ et $b > 1$, si $f(x)$ est $O(\log_b x)$, alors $f(x)$ est $O(\log_a x)$.

26. Donnez une estimation de grand O pour chacune de ces fonctions. Pour le fonction g dans votre estimation $f(x)$ est $O(g(x))$, utilisez un simple fonction g du plus petit ordre.

a) $(n^3 + n^2 \log n)(\log n + 1) + (17 \log n + 19)(n^3 + 2)$

b) $(2^n + n^2)(n^3 + 3^n)$

c) $(n^n + n2^n + 5^n)(n! + 5^n)$

27. Donnez une estimation de grand O pour chacune de ces fonctions. Pour le fonction g dans votre estimation que $f(x)$ est $O(g(x))$, utilisez un fonction simple g du plus petit ordre.

a) $n \log(n^2 + 1) + n^2 \log n$

b) $(n \log n + 1)^2 + (\log n + 1)(n^2 + 1)$

c) $n^{2^n} + n^{n^2}$

28. Pour chaque fonction de l'exercice 1, déterminez si cette fonction est (x) et si elle est (x).

29. Pour chaque fonction de l'exercice 2, déterminez si est (x^2) et si elle est (x^2).

30. Montrer que chacune de ces paires de fonctions est de même commande.

a) $3x + 7$, x

b) $2x^2 + x - 7$, x^2

c) $\lfloor x + 1/2 \rfloor$, x

d) $\log(x^2 + 1)$, $\log_2 x$

e) journal $_{10} x$, journal $_2 x$

31. Montrer que $f(x)$ est $(g(x))$ si et seulement si $f(x)$ est $O(g(x))$ et $g(x)$ est $O(f(x))$.

32. Montrer que si $f(x)$ et $g(x)$ sont des fonctions de l'ensemble des nombres réels à l'ensemble des nombres réels, alors $f(x)$ est $O(g(x))$ si et seulement si $g(x)$ est $(f(x))$.

33. Montrer que si $f(x)$ et $g(x)$ sont des fonctions de l'ensemble des nombres réels à l'ensemble des nombres réels, alors $f(x)$ est $(g(x))$ si et seulement s'il y a des constantes positives k, C_1, et C_2 tels que $C_1 |g(x)| \leq |f(x)| \leq C_2 |g(x)|$ quand-toujours $x > k$.

34. a) Montrer que $3x^2 + x + 1$ est $(3x^2)$ en trouvant directement les constantes k, C_1 et C_2 de l'exercice 33.

b) Exprimer la relation en partie (a) en utilisant une image montrant les fonctions $3x^2 + x + 1$, $C_1 \cdot 3x^2$, et $C_2 \cdot 3x^2$, et la constante k sur l' axe des x, où C_1, C_2 et k sont les constantes que vous avez trouvées dans la partie (a) pour montrer que $3x^2 + x + 1$ est $(3x^2)$.

35. Exprimez la relation $f(x)$ est $(g(x))$ *en* utilisant une image. Afficher les graphiques des fonctions $f(x)$, $C_1 |g(x)|$, et $C_2 |g(x)|$, ainsi que la constante k sur l' axe des x.

36. Expliquez ce que signifie pour une fonction d'être (1).

37. Expliquez ce que signifie pour une fonction d'être (1).

38. Donner une estimation grande- O du produit du premier n impair entiers positifs.

41. Supposons que $f(x)$ soit $O(g(x))$ où f et g sont in- fonctions de rainage et illimitées. Afficher ce journal $|f(x)|$ est $O(\log |g(x)|)$.

42. Supposons que $f(x)$ soit $O(g(x))$. S'ensuit-il que $2^{f(x)}$ est $O(2^{g(x)})$?

43. Soit $f_1(x)$ et $f_2(x)$ *des* fonctions de l'ensemble des réels nombres à l'ensemble des nombres réels positifs. Montrez que si $f_1(x)$ et $f_2(x)$ sont tous les deux $(g(x))$, où $g(x)$ est une fonction de l'ensemble des nombres réels à l'ensemble des réels positifs nombres, alors $f_1(x) + f_2(x)$ est $(g(x))$. Est-ce toujours vrai si $f_1(x)$ et $f_2(x)$ peuvent prendre des valeurs négatives?

44. Supposons que $f(x)$, $g(x)$ et $h(x)$ sont des fonctions telles que $f(x)$ est $(g(x))$ et $g(x)$ est $(h(x))$. Montrer que $f(x)$ est $(h(x))$.

45. Si $f_1(x)$ et $f_2(x)$ sont des fonctions de l'ensemble des positifs entiers à l'ensemble des nombres réels positifs et $f_1(x)$ et $f_2(x)$ sont les deux $(g(x))$, est $(f_1 - f_2)(x)$ aussi $(g(x))$?

Soit le prouver ou donner un contre-exemple.

46. Montrer que si $f_1(x)$ et $f_2(x)$ sont des fonctions de l'ensemble d'entiers positifs à l'ensemble des nombres réels et $f_1(x)$ est $(g_1(x))$ et $f_2(x)$ est $(g_2(x))$, alors $(f_1 f_2)(x)$ est $((g_1 g_2)(x))$.

47. Trouver les fonctions f et g *à* partir de l'ensemble des entiers positifs à l'ensemble des nombres réels tels que $f(n)$ n'est pas $O(g(n))$ et $g(n)$ n'est pas $O(f(n))$.

48. Exprimez la relation $f(x)$ est $(g(x))$ *en* utilisant une image. Vérifier les graphes des fonctions $f(x)$ et $Cg(x)$, et comme la constante k sur l'axe réel.

49. Montrer que si $f_1(x)$ est $(g_1(x))$, $f_2(x)$ est $(g_2(x))$, et $f_2(x) = 0$ et $g_2(x) = 0$ pour tous les nombres réels $x > 0$, alors $(f_1 / f_2)(x)$ est $((g_1 / g_2)(x))$.

50. Montrer que si $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x +$ *un* $_0$, où $a_0, a_1, \ldots, a_{n-1}$, et *un* $_n$ sont des nombres réels et $a_n = 0$, alors $f(x)$ est (x^n).

La notation Big- O, big-Theta et big-Omega peut être étendue aux fonctions dans plus d'une variable. Par exemple, ment $f(x, y)$ est $O(g(x, y))$ signifie qu'il existe des constantes C, k_1 et k_2 tels que $|f(x, y)| \leq C |g(x, y)|$ chaque fois que $x > k_1$ et $y > k_2$.

51. Définissez l'instruction $f(x, y)$ est $(g(x, y))$.

52. Définissez l'énoncé $f(x, y)$ est $(g(x, y))$.

53. Montrez que $(x^2 + xy + x \log y)^3$ est $O(x^6 y^3)$.

54. Montrez que $x^5 y^3 + x^4 y^4 + x^3 y^5$ est $(x^3 y^3)$.

55. Montrez que $\lfloor xy \rfloor$ est $O(xy)$.

56. Montrez que $\lceil xy \rceil$ est (xy).

57. (*Nécessite un calcul*) Montrez que si $c > d > 0$, alors n^d est $O(n^c)$, mais n^c n'est pas $O(n^d)$.

58. (*Nécessite un calcul*) Montrez que si $b > 1$ et c et d sont positifs, alors $(\log_b n)^c$ est $O(n^d)$, mais n^d n'est pas $O((\log_b n)^c)$.

Page 239

59. (*Nécessite un calcul*) Montrez que si d est positif et $b > 1$, alors n^d est $O(b^n)$ mais b^n n'est pas $O(n^d)$.

60. (*Calcul requis*) Montrer que si $c > b > 1$, alors b^n est $O(c^n)$ mais c^n n'est pas $O(b^n)$.

Les problèmes suivants concernent un autre type d'asymptotique notation, appelée notation **peu-** $\boldsymbol{o}$. Parce que la notation little- o est basé sur le concept de limites, une connaissance du calcul est nécessaires pour ces problèmes. On dit que $f(x)$ est $o(g(x))$ [lire $f(x)$ est «petit-oh» de $g(x)$], lorsque

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0 .$$

61. (*Nécessite un calcul*) Montrez que

a) x^2 est $o(x^3)$.

b) $x \log x$ est $o(x^2)$.

c) x^2 est $o(2^x)$.

d) $x^2 + x + 1$ n'est pas $o(x^2)$.

62. (*Nécessite un calcul*)

a) Montrer que si $f(x)$ et $g(x)$ sont des fonctions telles que $f(x)$ est $o(g(x))$ et c est une constante, alors $cf(x)$ est $o(g(x))$, où $(cf)(x) = cf(x)$.

69. (*Nécessite un calcul*) Montrez que si $f_1(x)$ est $O(g(x))$ et $f_2(x)$ est $o(g(x))$, alors $f_1(x) + f_2(x)$ est $O(g(x))$.

70. (*Nécessite calcul*) Soit H_n soit le n ième **nombre harmonique**

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} .$$

Montrez que H_n est $O(\log n)$. [*Indice:* établissez d'abord égalité

$$\sum_{j=2}^{n} \frac{1}{j} < \int_{1}^{n} \frac{1}{X} dx$$

en montrant que la somme des aires des rectangles de hauteur $1/j$ avec base de $j - 1$ à j, pour $j = 2, 3, \ldots, n$, est inférieure à l'aire sous la courbe $y = 1/x$ de 2 à n .]

$*$ **71.** Montrez que $n \log n$ est $O(\log n!)$.

72. Déterminez si $\log n!$ est $(n \log n)$. Justifiez votre

b) Montrer que si $f_1(x)$, $f_2(x)$ et $g(x)$ sont des fonctions tel que $f_1(x)$ est $o(g(x))$ et $f_2(x)$ est $o(g(x))$, alors $(f_1 + f_2)(x)$ est $o(g(x))$, où $(f_1 + f_2)(x) = f_1(x) + f_2(x)$.

63. (*Calcul requis*) Représente graphiquement que $x \log x$ est $o(x^2)$ en représentant graphiquement $x \log x$, x^2 et $x \log x / x^2$. Explique comment cette image montre que $x \log x$ est $o(x^2)$.

64. (*Calcul requis*) Exprimer la relation $f(x)$ est $o(g(x))$ *en* utilisant une image. Montrez les graphiques de $f(x)$, $g(x)$, et $f(x) / g(x)$.

∗ **65.** (*Nécessite un calcul*) Supposons que $f(x)$ soit $o(g(x))$. Est-ce que il s'ensuit que $2^{f(x)}$ est $o(2^{g(x)})$?

∗ **66.** (*Nécessite un calcul*) Supposons que $f(x)$ soit $o(g(x))$. Est-ce que il suit ce journal $|f(x)|$ est $o(\log |g(x)|)$?

67. (*Nécessite un calcul*) Les deux parties de cet exercice décrivent la relation entre la notation little- o et big- O .

a) Montrer que si $f(x)$ et $g(x)$ sont des fonctions telles que $f(x)$ est $o(g(x))$, alors $f(x)$ est $O(g(x))$.

b) Montrer que si $f(x)$ et $g(x)$ sont des fonctions telles que $f(x)$ est $O(g(x))$, alors il ne suit pas nécessairement que $f(x)$ est $o(g(x))$.

68. (*Nécessite un calcul*) Montrez que si $f(x)$ est un polynôme de le degré n et $g(x)$ est un polynôme de degré m où $m > n$, alors $f(x)$ est $o(g(x))$.

swer.

∗ **73.** Montrez ce journal $n!$ est supérieur à $(n \log n) / 4$ pour $n > 4$. [*Astuce:* Commencez par l'inégalité $n! > n(n-1)(n-2) \cdots \lceil n/2 \rceil$.]

Soit $f(x)$ et $g(x)$ *des* fonctions de l'ensemble des nombres réels bers à l'ensemble des nombres réels. Nous disons que la fonction tions f et g sont **asymptotique** et écrire $f(x) \sim g(x)$ si $\lim_{x \to \infty} f(x) / g(x) = 1$.

74. (*Nécessite un calcul*) Pour chacune de ces paires de fonctions, déterminer si f et g sont asymptotiques.

a) $f(x) = x^2 + 3x + 7$, $g(x) = x^2 + 10$

b) $f(x) = x^2 \log x$, $g(x) = x^3$

c) $f(x) = x^4 + \log(3x^8 + 7)$, $g(x) = (x^2 + 17x + 3)^2$

d) $f(x) = (x^3 + x^2 + x + 1)^4$, $g(x) = (x^4 + x^3 + x^2 + x + 1)^3$.

75. (*Nécessite un calcul*) Pour chacune de ces paires de fonctions, déterminer si f et g sont asymptotiques.

a) $f(x) = \log(x^2 + 1)$, $g(x) = \log x$

b) $f(x) = 2^{x+3}$, $g(x) = 2^{x+7}$

c) $f(x) = 2^{2^x}$, $g(x) = 2^{x^2}$

d) $f(x) = 2^{x^2+x+1}$, $g(x) = 2^{x^2+2x}$

Complexité des algorithmes

introduction

Quand un algorithme apporte-t-il une solution satisfaisante à un problème? Premièrement, il doit toujours produire la bonne réponse. La manière dont cela peut être démontré sera discutée au chapitre 5. Deuxièmement, il devrait être efficace. L'efficacité des algorithmes sera discutée dans cette section.

Comment analyser l'efficacité d'un algorithme? Une mesure de l'efficacité est le temps utilisé par un ordinateur pour résoudre un problème à l'aide de l'algorithme, lorsque les valeurs d'entrée sont d'une valeur spécifiée

Taille. Une deuxième mesure est la quantité de mémoire informatique requise pour implémenter l'algorithme lorsque les valeurs d'entrée ont une taille spécifiée.

De telles questions impliquent la **complexité** de **calcul** de l'algorithme. Une analyse du temps nécessaire pour résoudre un problème d'une taille particulière implique la **complexité temporelle** du algorithme. Une analyse de la mémoire de l'ordinateur requise implique la **complexité** de l' **espace** l'algorithme. La prise en compte de la complexité temporelle et spatiale d'un algorithme est essentielle lorsque des algorithmes sont mis en œuvre. Il est évidemment important de savoir si un algorithme produire une réponse en une microseconde, une minute ou un milliard d'années. De même, la mémoire requise doit être disponible pour résoudre un problème, de sorte que la complexité de l'espace doit être prise en compte.

Les considérations de complexité de l'espace sont liées aux structures de données particulières utilisées pour implémenter l'algorithme. Parce que les structures de données ne sont pas traitées en détail dans ce livre, l'espace la complexité ne sera pas prise en compte. Nous limiterons notre attention à la complexité du temps.

Complexité temporelle

La complexité temporelle d'un algorithme peut être exprimée en termes de nombre d'opérations utilisé par l'algorithme lorsque l'entrée a une taille particulière. Les opérations utilisées pour mesurer le temps la complexité peut être la comparaison d'entiers, l'addition d'entiers, la multiplication de entiers, la division d'entiers ou toute autre opération de base.

La complexité temporelle est décrite en termes de nombre d'opérations requises au lieu de réelles temps d'ordinateur en raison de la différence de temps nécessaire pour que différents ordinateurs exécutent opérations. De plus, il est assez compliqué de décomposer toutes les opérations en opérations de base sur les bits. que l'ordinateur utilise. De plus, les ordinateurs les plus rapides qui existent peuvent exécuter des opérations binaires (par exemple, ajouter, multiplier, comparer ou échanger deux bits) dans 10^{-11} seconde (10 picosecondes), mais les ordinateurs personnels peuvent nécessiter 10^{-8} seconde (10 nanosecondes), qui est 1000 fois plus long, pour faire les mêmes opérations.

Nous illustrons comment analyser la complexité temporelle d'un algorithme en considérant l'algorithme 1 de la section 3.1, qui trouve le maximum d'un ensemble fini d'entiers.

EXEMPLE 1 Décrire la complexité temporelle de l'algorithme 1 de la section 3.1 pour trouver l'élément maximal dans un ensemble fini d'entiers.

Solution: Le nombre de comparaisons sera utilisé comme mesure de la complexité temporelle du algorithme, car les comparaisons sont les opérations de base utilisées.

Pour trouver l'élément maximal d'un ensemble de n éléments, répertorié dans un ordre arbitraire, le le maximum temporaire est d'abord égal au terme initial dans la liste. Ensuite, après une comparaison $i \leq n$ a été fait pour déterminer que la fin de la liste n'est pas encore atteinte, le maximum et le deuxième terme sont comparés, mettant à jour le maximum temporaire à la valeur de le deuxième terme s'il est plus grand. Cette procédure se poursuit en utilisant deux comparaisons supplémentaires pour chaque terme de la liste - un $i \leq n$, pour déterminer que la fin de la liste n'a pas été atteinte et un autre max $< a_i$, pour déterminer s'il faut mettre à jour le maximum temporaire. Parce que deux des comparaisons sont utilisés pour chacune de la deuxième à la n ième éléments et une comparaison plus est utilisé pour quitter la boucle lorsque $i = n + 1$, exactement $2(n - 1) + 1 = 2n - 1$ comparaisons sont utilisées chaque fois que cet algorithme est appliqué. Par conséquent, l'algorithme pour trouver le maximum d'un ensemble de n éléments a une complexité temporelle (n), mesurée en termes de nombre de comparaisons utilisé. Notez que pour cet algorithme, le nombre de comparaisons est indépendant d'une entrée particulière de n nombres. ▲

Ensuite, nous analyserons la complexité temporelle des algorithmes de recherche.

EXEMPLE 2 Décrire la complexité temporelle de l'algorithme de recherche linéaire (spécifié comme Algortihm 2 dans Section 3.1).

Solution: Le nombre de comparaisons utilisé par l'algorithme 2 dans la section 3.1 sera considéré comme le mesure de la complexité temporelle. À chaque étape de la boucle de l'algorithme, deux comparaisons sont effectuées - un $i \leq n$, pour voir si la fin de la liste est atteinte et un $x \leq a_i$, pour comparer l'élément x avec un terme de la liste. Enfin, une autre comparaison $i \leq n$ est faite en dehors de la boucle. Par conséquent, si $x = a_i$, $2i + 1$ des comparaisons sont utilisées. Le plus de comparaisons, $2n + 2$, sont requis lorsque l'élément n'est pas dans la liste. Dans ce cas, $2n$ comparaisons sont utilisées pour déterminer que x n'est pas un_i, pour $i = 1, 2, ..., n$, une comparaison supplémentaire est utilisée pour quitter le boucle, et une comparaison est effectuée en dehors de la boucle. Donc, lorsque x n'est pas dans la liste, un total de $2n + 2$ des comparaisons sont utilisées. Par conséquent, une recherche linéaire nécessite *(n) des* comparaisons dans le pire des cas, parce que $2n + 2$ est (n). ▲

PIRE COMPLEXITÉ DE CAS Le type d'analyse de complexité effectué dans l'exemple 2 est le **pire** analyse de **cas** . Par la pire performance d'un algorithme, nous entendons le plus grand nombre de opérations nécessaires pour résoudre le problème donné en utilisant cet algorithme sur une entrée de taille spécifiée. L'analyse du pire des cas nous indique combien d'opérations un algorithme nécessite pour garantir qu'il produire une solution.

EXEMPLE 3 Décrire la complexité temporelle de l'algorithme de recherche binaire (spécifié comme algorithme 3 dans Section 3.1) en termes de nombre de comparaisons utilisées (et en ignorant le temps nécessaire pour calculer $m = \lfloor (i + j) / 2 \rfloor$ à chaque itération de la boucle dans l'algorithme).

Solution: pour simplifier, supposons qu'il y a $n = 2^k$ éléments de la liste $a_1, a_2, ..., a_n$, où k est un entier non négatif. Notez que $k = \log n$. (Si n, le nombre d'éléments dans la liste, n'est pas une puissance de 2, la liste peut être considérée comme faisant partie d'une liste plus 2^{k+1} éléments, où $2^k < n < 2^{k+1}$. Ici 2^{k+1} est la plus petite puissance de 2 supérieure à n.)

À chaque étape de l'algorithme, i et j, les emplacements du premier terme et du dernier terme de la liste restreinte à ce stade, sont comparés pour voir si la liste restreinte a plus d'un terme. Si $i < j$, une comparaison est effectuée pour déterminer si x est supérieur au terme moyen de la liste restreinte.

Au premier stade, la recherche est limitée à une liste de 2^{k-1} termes. Jusqu'à présent, deux comparaisons ont été utilisées. Cette procédure se poursuit en utilisant deux comparaisons à chaque étape pour restreindre la recherche d'une liste avec deux fois moins de termes. En d'autres termes, deux comparaisons sont utilisées au première étape de l'algorithme lorsque la liste a 2^k éléments, deux de plus lorsque la recherche a été réduit à une liste avec 2^{k-1} éléments, deux de plus lorsque la recherche a été réduite à une liste avec 2^{k-2} et ainsi de suite, jusqu'à ce que deux comparaisons soient utilisées lorsque la recherche a été réduite à un liste avec $2^1 = 2$ éléments. Enfin, quand un terme est laissé dans la liste, une comparaison nous dit que il n'y a plus de termes supplémentaires et une comparaison de plus est utilisée pour déterminer si ce terme est x.

Par conséquent, au plus $2k + 2 = 2 \log n + 2$ comparaisons sont nécessaires pour effectuer une recherche binaire lorsque la liste recherchée a 2^k éléments. (Si n n'est pas une puissance de 2, la liste d'origine est développée à une liste avec 2^{k+1} termes, où $k = \lfloor \log n \rfloor$, et la recherche nécessite au plus $2 \lceil \log n \rceil + 2$ comparaisons.) Il s'ensuit que dans le pire des cas, la recherche binaire nécessite des comparaisons $O(\log n)$. Notez que dans le pire des cas, 2 comparaisons $\log n + 2$ sont utilisées par la recherche binaire. D'où le la recherche binaire utilise des comparaisons $(\log n)$ dans le pire des cas, car $2 \log n + 2 = (\log n)$. De cette analyse, il s'ensuit que dans le pire des cas, l'algorithme de recherche binaire est plus efficace que l'algorithme de recherche linéaire, parce que nous savons par l'exemple 2 que l'algorithme de recherche linéaire a *(n) la* complexité temporelle la plus défavorable. ▲

COMPLEXITÉ MOYENNE DES CAS Un autre type important d'analyse de la complexité, outre l'analyse du pire des cas est appelée analyse du **cas moyen** . Le nombre moyen d'opérations utilisé pour résoudre le problème sur toutes les entrées possibles d'une taille donnée se trouve dans ce type d'analyse. Moyenne- L'analyse de la complexité du temps des cas est généralement beaucoup plus compliquée que l'analyse du pire des cas.

Cependant, l'analyse de cas moyen pour l'algorithme de recherche linéaire peut être effectuée sans difficulté, comme le montre l'exemple 4.

EXEMPLE 4 Décrire les performances de cas moyen de l'algorithme de recherche linéaire en termes de moyenne nombre de comparaisons utilisées, en supposant que l'entier x est dans la liste et qu'il est tout aussi probable que x est dans n'importe quelle position.

Solution: Par hypothèse, l'entier x est l'un des entiers $a_1, a_2, \ldots, a_n$ de la liste. Si x est le premier terme a_1 de la liste, trois comparaisons sont nécessaires, une $i \leq n$ pour déterminer si la fin de la liste est atteinte, un $x = a_i$ pour comparer x et le premier terme, et un $i \leq n$ extérieur la boucle. Si x est le deuxième terme a_2 de la liste, deux comparaisons supplémentaires sont nécessaires, de sorte qu'un total cinq comparaisons sont utilisées. En général, si x est le i ème terme de la liste a_i, deux comparaisons seront être utilisé à chacune des i étapes de la boucle, et une à l'extérieur de la boucle, de sorte qu'un total de $2i + 1$ des comparaisons sont nécessaires. Par conséquent, le nombre moyen de comparaisons utilisées est égal à

$$\frac{3 + 5 + 7 + \cdots + (2n + 1)}{n} = \frac{2(1 + 2 + 3 + \cdots + n) + n}{n}.$$

En utilisant la formule de la ligne 2 du tableau 2 de la section 2.4 (et voir l'exercice 37 (b) de la section 2.4),

$$1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2}.$$

Par conséquent, le nombre moyen de comparaisons utilisées par l'algorithme de recherche linéaire (lorsque x est connu pour figurer dans la liste) est

$$\frac{2[n(n + 1)/2]}{n} + 1 = n + 2,$$

qui est *(n)* . ▲

Remarque: Dans l'analyse de l'exemple 4, nous avons supposé que x figure dans la liste recherchée. C'est aussi possible de faire une analyse de cas moyen de cet algorithme lorsque x peut ne pas être dans la liste (voir Exercice 23).

Remarque: Bien que nous ayons compté les comparaisons nécessaires pour déterminer si nous avons atteint la fin d'une boucle, ces comparaisons ne sont souvent pas comptées. À partir de ce moment, nous ignorer ces comparaisons.

PIRE COMPLEXITÉ DE DEUX ALGORITHMES DE TRI Nous analysons la dans le pire des cas, la complexité du tri à bulles et du tri par insertion dans les exemples 5 et 6.

EXEMPLE 5 Quelle est la complexité la plus défavorable du tri à bulles en termes de nombre de comparaisons fait?

Solution: le tri à bulles décrit avant l'exemple 4 de la section 3.1 trie une liste en effectuant une séquence de passe à travers la liste. Lors de chaque passage, le tri à bulles compare successivement éléments adjacents, en les échangeant si nécessaire. Lorsque le i ème passage commence, le $i - 1$ plus grand les éléments sont garantis dans les bonnes positions. Pendant cette passe, $n - i$ comparaisons sont utilisé. Par conséquent, le nombre total de comparaisons utilisées par le tri à bulles pour ordonner une liste de n éléments est

$$(n - 1) + (n - 2) + \cdots + 2 + 1 = \frac{(n - 1)n}{2}$$

en utilisant une formule de sommation de la ligne 2 du tableau 2 de la section 2.4 (et de l'exercice 37 (b) Section 2.4). Notez que le tri à bulles utilise toujours autant de comparaisons, car il continue même si la liste est complètement triée à une étape intermédiaire. Par conséquent, le le tri à bulles utilise $(n - 1) n / 2$ comparaisons, il a donc (n^2) *la* complexité la plus défavorable en termes de le nombre de comparaisons utilisées. ▲

EXEMPLE 6 Quelle est la complexité la plus défavorable du tri par insertion en termes de nombre de comparaisons fait?

Solution: le tri par insertion (décrit à la section 3.1) insère le j ème élément dans le bon positionner parmi les premiers $j - 1$ éléments déjà placés dans le bon ordre. Cela fait ceci en utilisant une technique de recherche linéaire, en comparant successivement le j ème élément avec des éléments successifs termes jusqu'à ce qu'un terme supérieur ou égal à lui soit trouvé ou qu'il compare *un* $_j$ avec lui-même et s'arrête car *un* $_j$ n'est pas moins que lui-même. Par conséquent, dans le pire des cas, j *des* comparaisons sont nécessaires pour insérer le j ème élément dans la position correcte. Par conséquent, le nombre total de comparaisons utilisé par le tri par insertion pour trier une liste de n éléments est

$$2 + 3 + \cdots + n = \frac{n(n+1)}{2} - 1,$$

en utilisant la formule de sommation pour la somme des nombres entiers consécutifs à la ligne 2 du tableau 2 de Section 2.4 (et voir exercice 37 (b) de la section 2.4), et notant que le premier terme, 1, est manquant dans cette somme. Notez que le tri par insertion peut utiliser beaucoup moins de comparaisons si le plus petit les éléments ont commencé à la fin de la liste. Nous concluons que le tri par insertion a le pire des cas complexité (n^2). ▲

Dans les exemples 5 et 6, nous avons montré que le tri à bulles et le tri par insertion pire complexité du temps (n^2). Cependant, les algorithmes de tri les plus efficaces peuvent trier n éléments en temps $O(n \log n)$, comme nous le montrerons dans les sections 8.3 et 11.1 en utilisant les techniques que nous développons ces sections. À partir de là, nous supposerons que le tri de n éléments peut être effectué dans $O(n \log n)$ temps.

Complexité de la multiplication matricielle

La définition du produit de deux matrices peut être exprimée comme un algorithme de calcul le produit de deux matrices. Supposons que $\mathbf{C} = [c_{ij}]$ est la matrice $m \times n$ qui est le produit de la $m \times k$ matrice $\mathbf{A} = [a_{ij}]$ et la $k \times n$ matrice $\mathbf{B} = [b_{ij}]$. L'algorithme basé sur la définition du produit matriciel est exprimé en pseudocode dans l'algorithme 1.

ALGORITHME 1 **Multiplication matricielle.**

```
multiplication de matrices de procédures ( A , B : matrices)
pour i : = 1 à m
    pour j : = 1 à n
        c_ij : = 0
        pour q : = 1 à k
            c_ij : = c_ij + a_iq b_qj
retour C { C = [ c_ij ] est le produit de A et B }
```

Nous pouvons déterminer la complexité de cet algorithme en termes de nombre d'ajouts et multiplications utilisées.

EXEMPLE 7 Combien d'ajouts d'entiers et de multiplications d'entiers sont utilisés par l'algorithme 1 pour multiplier deux matrices $n \times n$ avec des entrées entières?

Solution: Il y a n^2 entrées dans le produit de **A** et **B.** Pour trouver chaque entrée, il faut un total de n multiplications et $n - 1$ additions. Par conséquent, un total de n^3 multiplications et $n^2 (n - 1)$ des ajouts sont utilisés. ▲

Étonnamment, il existe des algorithmes plus efficaces pour la multiplication matricielle que ceux Algorithme 1. Comme le montre l'exemple 7, en multipliant deux $n \times n$ matrices directement à partir de la définition nécessite $O(n^3)$ multiplications et additions. En utilisant d'autres algorithmes, deux matrices $n \times n$ peuvent être multiplié en utilisant $O(n^{\sqrt{7}})$ multiplications et ajouts. (Les détails de ces algorithmes peuvent être trouvé dans [CoLeRiSt09].)

Nous pouvons également analyser la complexité de l'algorithme que nous avons décrit au chapitre 2 pour le calcul le produit booléen de deux matrices, que nous affichons comme algorithme 2.

ALGORITHME 2 Le produit booléen des matrices zéro-un.

procédure *Produit booléen de matrices zéro-un* (**A** , **B** : matrices zéro-un)
pour $i := 1$ **à** m
  pour $j := 1$ **à** n
    $c_{ij} := 0$
    pour $q := 1$ **à** k
      $c_{ij} := c_{ij} \vee (a_{iq} \wedge b_{qj})$
return C { $\mathbf{C} = [c_{ij}]$ est le produit booléen de **A** et **B** }

Le nombre d'opérations binaires utilisées pour trouver le produit booléen de deux matrices $n \times n$ peut être facilement déterminé.

EXEMPLE 8 Combien d'opérations binaires sont utilisées pour trouver $\mathbf{A} \odot \mathbf{B}$, où **A** et **B** sont $n \times n$ matrices zéro – un?

Solution: Il y a n^2 entrées dans $\mathbf{A} \odot \mathbf{B}$. En utilisant l'algorithme 2, un total de n *OU* s et n *ET* s sont utilisé pour trouver une entrée de $\mathbf{A} \odot \mathbf{B}$. Par conséquent, des opérations de $2n$ bits sont utilisées pour trouver chaque entrée. Donc, $2n^3$ opérations de bits sont nécessaires pour calculer $\mathbf{A} \odot \mathbf{B}$ en utilisant l' algorithme 2. ▲

MULTIPLICATION À CHAÎNE MATRICE Il existe un autre problème important concernant la complexité de la multiplication des matrices. Comment la **chaîne matricielle** $\mathbf{A}_1 \mathbf{A}_2 \cdots \mathbf{A}_n$ *doit-elle* être commis en utilisant le moins de multiplications d'entiers, où $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ sont $m_1 \times m_2$, $m_2 \times m_3, \ldots, m_n \times m_{n+1}$ matrices, respectivement, et chacune a des entiers comme entrées? (Parce que la matrice la multiplication est associative, comme le montre l'exercice 13 de la section 2.6, l'ordre des tiplication utilisée ne change pas le produit.) Notez que $m_1 m_2 m_3$ multiplications d'entiers sont effectuées pour multiplier une matrice $m_1 \times m_2$ et une matrice $m_2 \times m_3$ en utilisant l'algorithme 1. L'exemple 9 illustre ce problème.

EXEMPLE 9 Dans quel ordre les matrices $\mathbf{A}_1$, $\mathbf{A}_2$ et $\mathbf{A}_3$ - où $\mathbf{A}_1$ est 30×20, $\mathbf{A}_2$ est 20×40, et **Un** $_3$ est 40×10, tous avec des entrées entières - être multiplié pour utiliser le moins de multiplications d'entiers?

Solution: Il existe deux façons de calculer $\mathbf{A}_1 \mathbf{A}_2 \mathbf{A}_3$. Ce sont $\mathbf{A}_1(\mathbf{A}_2 \mathbf{A}_3)$ et $(\mathbf{A}_1 \mathbf{A}_2)\mathbf{A}_3$.

Si $\mathbf{A}_2$ et $\mathbf{A}_3$ sont d'abord multipliés, un total de $20 \cdot 40 \cdot 10 = 8000$ multiplications d'intégra- gers sont utilisés pour obtenir la matrice 20×10 $\mathbf{A}_2 \mathbf{A}_3$. Ensuite, pour multiplier $\mathbf{A}_1$ et $\mathbf{A}_2 \mathbf{A}_3$, il faut $30 \cdot 20 \cdot 10 = 6000$ multiplications. Par conséquent, un total de

$$8000 + 6000 = 14\,000$$

des multiplications sont utilisées. En revanche, si $\mathbf{A}_1$ et $\mathbf{A}_2$ sont d'abord multipliés, alors 30 · 20 · 40 = 24 , 000 multiplications sont utilisés pour obtenir la matrice 30 x 40 $\mathbf{A}_1\mathbf{A}_2$. Ensuite, pour multiplier $\mathbf{A}_1\mathbf{A}_2$ et $\mathbf{A}_3$ nécessite 30 · 40 · 10 = 12 000 multiplications.Par conséquent, un total de

24.000 + 12.000 = 36.000

des multiplications sont utilisées.

De toute évidence, la première méthode est plus efficace. ▲

Nous reviendrons sur ce problème dans l'exercice 57 de la section 8.1.Algorithmes pour déterminer la manière la plus efficace d'effectuer la multiplication matrice-chaîne est discutée dans [CoLeRiSt09].

Paradigmes algorithmiques

Dans la section 3.1, nous avons introduit la notion de base d'un algorithme.Nous avons fourni des exemples de nombreux différents algorithmes, y compris des algorithmes de recherche et de tri.Nous avons également introduit le concept d'un algorithme gourmand, donnant des exemples de plusieurs problèmes qui peuvent être résolus par une rithms. Les algorithmes gourmands fournissent un exemple de **paradigme algorithmique** , c'est-à-dire un approche basée sur un concept particulier qui peut être utilisé pour construire des algorithmes pour résoudre un variété de problèmes.

Dans ce livre, nous allons construire des algorithmes pour résoudre de nombreux problèmes différents basés sur un variété de paradigmes algorithmiques, y compris les paradigmes algorithmiques les plus largement utilisés.Celles-ci les paradigmes peuvent servir de base à la construction d'algorithmes efficaces pour résoudre un large éventail de problèmes.

Certains des algorithmes que nous avons déjà étudiés sont basés sur un paradigme algorithmique connu comme force brute, que nous décrirons dans cette section. Paradigmes algorithmiques, étudiés plus tard dans ce livre, comprennent des algorithmes de division et de conquête étudiés dans le chapitre 8, la programmation dynamique, également étudié au chapitre 8, le retour en arrière, étudié au chapitre 10, et les algorithmes probabilistes, étudié au chapitre 7. Il existe de nombreux paradigmes algorithmiques importants en plus de ceux décrits dans ce livre. Consultez des livres sur la conception d'algorithmes tels que [KlTa06] pour en savoir plus à leur sujet.

ALGORITHMES DE BRUTE-FORCE La force **brutale** est un algorithme important et basique paradigme. Dans un **algorithme de force brute** , un problème est résolu de la manière la plus simple sur la base de l'énoncé du problème et des définitions des termes.Les algorithmes de force brute sont conçu pour résoudre les problèmes sans tenir compte des ressources informatiques nécessaires.Par exemple, dans certains algorithmes de force brute, la solution à un problème est trouvée en examinant tous les solution, à la recherche du meilleur possible.En général, les algorithmes de force brute sont des approches naïves pour résoudre des problèmes qui ne profitent d'aucune structure particulière du problème ou intelligent des idées.

Notez que l'algorithme 1 de la section 3.1 pour trouver le nombre maximum dans une séquence est un algorithme de force brute, car il examine chacun des n nombres dans une séquence pour trouver le durée maximale. L'algorithme pour trouver la somme de n nombres en ajoutant un supplémentaire nombre à la fois est également un algorithme de force brute, tout comme l'algorithme de multiplication matricielle basé sur sa définition (algorithme 1). Les bulles, les insertions et les sélections (décrites dans La section 3.1 des algorithmes 4 et 5 et de l'exercice 42, respectivement) est également considérée comme algorithmes de force brute; ces trois algorithmes de tri sont des approches simples beaucoup moins efficace que d'autres algorithmes de tri tels que le tri par fusion et le tri rapide discuté dans les chapitres 5 et 8.

Bien que les algorithmes de force brute soient souvent inefficaces, ils sont souvent très utiles.Une brute-algorithme de force peut être en mesure de résoudre des cas pratiques de problèmes, en particulier lorsque l'entrée

n'est pas trop grand, même s'il n'est pas pratique d'utiliser cet algorithme pour des entrées plus importantes.En outre, lors de la conception de nouveaux algorithmes pour résoudre un problème, le but est souvent de trouver un nouvel algorithme qui est plus efficace qu'un algorithme de force brute.Un tel problème de ce type est décrit dans l'exemple 10.

EXEMPLE 10 Construire un algorithme de force brute pour trouver la paire de points la plus proche dans un ensemble de n points dans l'avion et fournir une estimation big- *O du* pire cas pour le nombre d'opérations de bits utilisées par le algorithme.

Solution: Supposons que l'on nous donne en entrée les points $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$. Rappel que la distance entre (x_i, y_i) et (x_j, y_j) est $(x_j - x_i)^2 + (y_j - y_i)^2$. Une algo-rithm peut trouver la paire la plus proche de ces points en calculant les distances entre toutes les paires de les n points et déterminer la plus petite distance. (Nous pouvons faire une petite simplification pour rendre le calcul plus facile; on peut calculer le carré de la distance entre des paires de points pour trouver la paire la plus proche, plutôt que la distance entre ces points. Nous pouvons le faire parce que le carré de la distance entre une paire de points est le plus petit lorsque la distance entre ces points points est le plus petit.)

ALGORITHME 3 Algorithme de force brute pour la paire de points la plus proche.

procédure *paire la plus proche* ($(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$: paires de nombres réels)
$min = \infty$
pour $i := 2$ **à** n
  pour $j := 1$ **à** $i - 1$
    si $(x_j - x_i)^2 + (y_j - y_i)^2 < min$ **alors**
      $min := (x_j - x_i)^2 + (y_j - y_i)^2$
      paire la plus proche $:= ((x_i, y_i), (x_j, y_j))$
retourner la *paire la plus proche*

Pour estimer le nombre d'opérations utilisées par l'algorithme, notons d'abord qu'il existe $n(n - 1)/2$ paires de points $((x_i, y_i), (x_j, y_j))$ que nous parcourons (comme le lecteur devrait vérifier). Pour chaque paire, nous calculons $(x_j - x_i)^2 + (y_j - y_i)^2$, comparons-le avec la valeur actuelle de *min*, et si elle est inférieure à *min,* remplacer la valeur actuelle de *min* par cette nouvelle valeur. Ça suit que cet algorithme utilise des opérations (n^2), en termes d'opérations arithmétiques et de comparaisons.

Dans le chapitre 8, nous allons concevoir un algorithme qui détermine la paire de points la plus proche une fois donné n points dans le plan comme entrée ayant la complexité $O(n \log n)$ *dans le* pire des cas. La découverte originale d'un tel algorithme, beaucoup plus efficace que l'approche par force brute, était considérée comme surprenant. ▲

Comprendre la complexité des algorithmes

Le tableau 1 présente une terminologie courante utilisée pour décrire la complexité temporelle des algorithmes. Par exemple, un algorithme qui trouve le plus grand des 100 premiers termes d'une liste de n éléments en appliquant l'algorithme 1 à la séquence des 100 premiers termes, où n est un entier avec $n \geq 100$, a **une complexité constante** car il utilise 99 comparaisons quel que soit n (comme le lecteur peut vérifier). L'algorithme de recherche linéaire a **linéaire** (pire cas ou cas moyen) **complexité** et l'algorithme de recherche binaire a une **complexité logarithmique** (pire des cas) **.** Beaucoup les algorithmes importants ont $n \log n$, ou une **complexité linéithmique** (pire des cas), comme la fusion tri, que nous présenterons au chapitre 4. (Le mot *linéarithmique* est une combinaison des mots *linéaire* et log *arithmiques* .)

TABLEAU 1 Terminologie couramment utilisée pour le Complexité des algorithmes.

Complexité	*Terminologie*
(1)	Complexité constante
$(\log n)$	Complexité logarithmique
(n)	Complexité linéaire
$(n \log n)$	Complexité linéarithmique
(n^b)	Complexité polynomiale
(b^n), où $b > 1$	Complexité exponentielle
$(n!)$	Complexité factorielle

Un algorithme a **une complexité polynomiale** s'il a une complexité (n^b), où b est un entier avec $b \geq 1$. Par exemple, l'algorithme de tri à bulles est un algorithme à temps polynomial car il utilise des comparaisons (n^2) dans le pire des cas. Un algorithme a **une complexité exponentielle** s'il

a une complexité temporelle (b^n), où $b > 1$. L'algorithme qui détermine si un composé
proposition en n variables est satisfiable en vérifiant toutes les affectations possibles des variables de vérité
est un algorithme à complexité exponentielle, car il utilise (2^n) opérations. Enfin, un
l'algorithme a une **complexité factorielle** s'il a $(n!)$ *une* complexité temporelle. L'algorithme qui trouve tout
les commandes qu'un vendeur itinérant pourrait utiliser pour visiter n villes a une complexité factorielle; nous allons
discutez de cet algorithme au chapitre 9.

TRAÇABILITÉ Un problème qui peut être résolu en utilisant un algorithme avec le pire des cas polynomiaux
la complexité est appelée **traitable** , car on s'attend à ce que l'algorithme produise le
solution au problème pour une entrée de taille raisonnable dans un temps relativement court. Cependant, si le
polynôme dans la grande estimation a un degré élevé (comme le degré 100) ou si les coefficients
sont extrêmement volumineux, l'algorithme peut prendre un temps extrêmement long pour résoudre le problème.
Par conséquent, qu'un problème peut être résolu en utilisant un algorithme avec le pire des cas polynomiaux
la complexité temporelle n'est pas une garantie que le problème peut être résolu dans un délai raisonnable
pour des valeurs d'entrée même relativement petites. Heureusement, dans la pratique, le degré et les coefficients de
les polynômes dans ces estimations sont souvent petits.

La situation est bien pire pour les problèmes qui ne peuvent pas être résolus en utilisant un algorithme avec
pire complexité polynomiale temporelle. Ces problèmes sont appelés **insolubles** . Habituellement, mais pas
toujours, un temps extrêmement long est nécessaire pour résoudre le problème dans les pires cas
même de petites valeurs d'entrée. Dans la pratique, cependant, il existe des situations où un algorithme avec un
une certaine complexité temporelle dans le pire des cas peut résoudre un problème beaucoup plus rapidement pour la plupart
cas que pour son pire des cas. Lorsque nous sommes disposés à autoriser ce nombre, peut-être petit,
des cas peuvent ne pas être résolus dans un délai raisonnable, la complexité temporelle moyenne des cas est
une meilleure mesure du temps qu'un algorithme prend pour résoudre un problème. Beaucoup de problèmes importants
dans l'industrie sont considérés comme insolubles, mais peuvent être pratiquement résolus pour pratiquement tous les
apport qui se posent dans la vie quotidienne. Une autre façon de traiter les problèmes insolubles lorsqu'ils surviennent
dans les applications pratiques, c'est qu'au lieu de chercher des solutions exactes à un problème,
des solutions sont recherchées. Il se peut que des algorithmes rapides existent pour trouver de telles so-
lutions, peut-être même avec la garantie qu'elles ne diffèrent pas beaucoup d'une solution exacte.

Certains problèmes existent même pour lesquels il peut être démontré qu'aucun algorithme n'existe pour résoudre
leur. Ces problèmes sont appelés **insolubles** (par opposition aux problèmes **résolubles** qui peuvent être
résolu à l'aide d'un algorithme). La première preuve de l'existence de problèmes insolubles a été fournie par
le grand mathématicien et informaticien anglais Alan Turing quand il a montré que le
l'arrêt du problème est insoluble. Rappelons que nous avons prouvé que le problème de l'arrêt est insoluble dans
Section 3.1. (Une biographie d'Alan Turing et une description de certains de ses autres travaux peuvent être
trouvé dans le chapitre 13.)

P VERSUS NP L'étude de la complexité des algorithmes va bien au-delà de ce que nous pouvons
décrire ici. Notez, cependant, que de nombreux problèmes résolubles auraient la propriété
qu'aucun algorithme avec une complexité temporelle polynomiale dans le pire des cas ne les résout, mais qu'une solution,
si elle est connue, peut être vérifiée en temps polynomial. Problèmes pour lesquels une solution peut être vérifiée
en temps polynomial appartiendraient à la **classe NP** (les problèmes traitables appartiendraient à
classe P). L'abréviation NP signifie temps *polynomial non déterministe* . La satisfiabilité
Le problème, discuté dans la section 1.3, est un exemple de problème NP - nous pouvons rapidement vérifier que
une affectation de valeurs de vérité aux variables d'une proposition composée le rend vrai, mais pas
Un algorithme de temps polynomial a été découvert pour trouver une telle affectation de valeurs de vérité.
(Par exemple, une recherche exhaustive de toutes les valeurs de vérité possibles nécessite (2^n) opérations sur les bits
où n est le nombre de variables dans la proposition composée.)

Il existe également une classe importante de problèmes, appelés problèmes **NP-complets** , avec
propriété que si l'un de ces problèmes peut être résolu par un algorithme de temps du pire cas polynomial,
tous les problèmes de la classe NP peuvent alors être résolus par des algorithmes polynomiaux du pire des cas.
Le problème de satisfiabilité est également un exemple de problème NP-complet. C'est un problème NP
et si un algorithme de temps polynomial pour le résoudre était connu, il y aurait du temps polynomial
des algorithmes pour tous les problèmes connus dans cette classe de problèmes (et il existe de nombreux
problèmes dans cette classe). Cette dernière affirmation découle du fait que chaque problème dans NP
peut être réduit en temps polynomial au problème de satisfiabilité. Bien que plus de 3000 NP-
des problèmes complets sont maintenant connus, le problème de satisfiabilité a été le premier
NP-complet. Le théorème qui affirme cela est connu comme le **théorème de Cook-Levin** après Stephen
Cook et Leonid Levin, qui l'ont prouvé indépendamment au début des années 1970.

Le **problème P versus NP** demande si NP, la classe de problèmes pour laquelle il est possible
pour vérifier les solutions en temps polynomial, est égal à P, la classe des problèmes traitables Si P = NP, il y a
seraient des problèmes qui ne peuvent pas être résolus en temps polynomial, mais dont les solutions pourraient
être vérifiée en temps polynomial. Le concept d'exhaustivité de NP est utile dans les recherches visant
à résoudre le problème P par rapport à NP, car les problèmes NP-complets sont les problèmes de NP
considéré comme le plus susceptible de ne pas être en P, car chaque problème de NP peut être réduit à un NP complet
problème en temps polynomial. Une grande majorité des informaticiens théoriques pensent que
P = NP, ce qui signifierait qu'aucun problème NP-complet ne peut être résolu en temps polynomial.
L'une des raisons de cette croyance est que, malgré des recherches approfondies, personne n'a réussi à montrer que
P = NP. En particulier, personne n'a été en mesure de trouver un algorithme avec le pire temps polynomial

complexité qui résout tout problème NP-complet. Le problème P versus NP est l'un des plus célèbres problèmes non résolus dans les sciences mathématiques (qui incluent l'ordinateur théorique science). Il s'agit de l'un des sept problèmes connus du Prix du Millénaire, dont six ne sont toujours pas résolus. Un prix de 1 $, 000 , 000 est offert par l'Institut Clay mathématiques pour sa solution.

STEPHEN COOK (NÉ EN 1939) Stephen Cook est né à Buffalo où son père travaillait comme industriel chimiste et a enseigné des cours universitaires. Sa mère a enseigné des cours d'anglais dans un collège communautaire. En lycée Cook a développé un intérêt pour l'électronique grâce à son travail avec un célèbre inventeur local connu pour inventant le premier stimulateur cardiaque implantable.

Cook était un majeur en mathématiques à l'Université du Michigan, diplômé en 1961. Il a fait des études supérieures à Harvard, où il a obtenu une maîtrise en 1962 et un doctorat. en 1966. Cook a été nommé professeur adjoint au Département de mathématiques de l'Université de Californie à Berkeley en 1966. Il n'a pas obtenu de permanence là, peut-être parce que les membres du département de mathématiques n'ont pas trouvé son travail sur ce qui est maintenant considéré comme l'un des domaines les plus importants de l'informatique théorique présentant un intérêt suffisant. En 1970, il s'est joint à l'Université de Toronto en tant que professeur adjoint, occupant un poste conjoint au Computer Département des sciences et Département des mathématiques. Il est resté à l'Université de Toronto, où il a été nommé Professeur d'université en 1985.

Cook est considéré comme l'un des fondateurs de la théorie de la complexité informatique. Son article de 1971 «La complexité du théorème Proving Procedures »a formalisé les notions de NP-complétude et de réduction du temps polynomial, a montré que les problèmes de NP-complet existent en montrant que le problème de satisfiabilité est un tel problème, et introduit le problème notoire de P contre NP.

Cook a reçu de nombreux prix, dont le prix Turing de 1982. Il est marié et a deux fils. Parmi ses intérêts figurent jouer du violon et des voiliers de course.

Pour plus d'informations sur la complexité des algorithmes, consultez les références, notamment [CoLeRiSt09], pour cette section répertoriée à la fin de ce livre.(Aussi, pour une discussion plus formelle de la complexité de calcul en termes de machines de Turing, voir la section 13.5.)

CONSIDÉRATIONS PRATIQUES Notez qu'une grande estimation de la complexité temporelle d'un l'algorithme exprime comment le temps nécessaire pour résoudre le problème augmente à mesure que l'entrée augmente en taille. En pratique, la meilleure estimation (c'est-à-dire avec la plus petite fonction de référence) qui peut être montré est utilisé. Cependant, les grandes estimations de la complexité temporelle ne peuvent pas être directement traduites en le temps réel utilisé par l'ordinateur. L'une des raisons est qu'une grande estimation $f(n)$ est $(g(n))$, où $f(n)$ est la complexité temporelle d'un algorithme et $g(n)$ est une fonction de référence, signifie que $C_1 g(n) \leq f(n) \leq C_2 g(n)$ lorsque $n > k$, où C_1 , C_2 et k sont des constantes. Donc sans connaissant les constantes C_1 , C_2 et k dans l'inégalité, cette estimation ne peut pas être utilisée pour déterminer une borne inférieure et une borne supérieure sur le nombre d'opérations utilisées dans le pire des cas. Comme remarqué précédemment, le temps nécessaire à une opération dépend du type d'opération et de la ordinateur utilisé. Souvent, au lieu d'une grande estimation de la complexité temporelle un algorithme, nous avons seulement une estimation big- O . Notez qu'une estimation big- O sur la complexité temporelle d'un algorithme fournit une limite supérieure, mais pas inférieure, sur le temps le plus défavorable requis pour l'algorithme en fonction de la taille d'entrée. Néanmoins, pour plus de simplicité, nous utiliserons souvent big- O estime lors de la description de la complexité temporelle des algorithmes, avec la compréhension ces grandes estimations fourniraient plus d'informations.

Le tableau 2 affiche le temps nécessaire pour résoudre des problèmes de différentes tailles avec un algorithme utilisant le nombre indiqué n d'opérations binaires, en supposant que chaque opération binaire prend 10^{-11} secondes, un estimation raisonnable du temps requis pour un fonctionnement en bits en utilisant les ordinateurs les plus rapides disponibles aujourd'hui. Les périodes de plus de 10^{100} ans sont indiquées par un astérisque. À l'avenir, ces temps diminuera avec le développement d'ordinateurs plus rapides. Nous pouvons utiliser les temps indiqués dans le tableau 2 pour voir s'il est raisonnable de s'attendre à une solution à un problème d'une taille spécifiée en utilisant un algorithme avec une complexité temporelle connue dans le pire des cas lorsque nous exécutons cet algorithme sur un ordinateur moderne. Notez que nous ne pouvons pas déterminer le temps exact qu'un ordinateur utilise pour résoudre un problème avec l'entrée de une taille particulière en raison d'une multitude de problèmes impliquant le matériel informatique et le particulier implémentation logicielle de l'algorithme.

Il est important d'avoir une estimation raisonnable du temps qu'il faudra à un ordinateur pour résoudre un problème. Par exemple, si un algorithme nécessite environ 10 heures, il peut être utile de passer le temps (et l'argent) requis pour résoudre ce problème. Mais, si un algorithme nécessite environ 10 milliards d'années pour résoudre un problème, il serait déraisonnable d'utiliser les ressources implémenter cet algorithme. L'un des phénomènes les plus intéressants de la technologie moderne est la augmentation considérable de la vitesse et de l'espace mémoire des ordinateurs. Un autre facteur important qui réduit le temps nécessaire pour résoudre les problèmes sur les ordinateurs est le **traitement parallèle** , qui est la technique consistant à exécuter simultanément des séquences d'opérations.

Des algorithmes efficaces, y compris la plupart des algorithmes à complexité temporelle polynomiale, bénéficient la plupart des améliorations technologiques importantes. Cependant, ces améliorations technologiques

TABLEAU 2 **Le temps de l'ordinateur utilisé par les algorithmes.**

Taille du problème	***Opérations sur les bits utilisées***					
n	$\log n$	n	$n \log n$	n^2	2^n	$n!$

dix	3×10^{-11} s	10 à 10 s	3×10^{-10} s	10^{-9} s	10^{-8} s	3×10^{-7} s
10^2	7×10^{-11} s	10^{-9} s	7×10^{-9} s	10^{-7} s	4×10^{11} ans	*
10^3	1.0×10^{-10} s	10^{-8} s	1×10^{-7} s	10^{-5} s	*	*
10^4	1.3×10^{-10} s	10^{-7} s	1×10^{-6} s	10^{-3} s	*	*
10^5	1.7×10^{-10} s	10^{-6} s	2×10^{-5} s	0.1 s	*	*
10^6	2×10^{-10} s	10^{-5} s	2×10^{-4} s	0.17 min	*	*

offrent peu d'aide pour surmonter la complexité des algorithmes de temps exponentiel ou factoriel complexité. En raison de la vitesse de calcul accrue, de l'augmentation de la mémoire de l'ordinateur et l'utilisation d'algorithmes qui tirent parti du traitement parallèle, de nombreux problèmes jugées impossibles à résoudre il y a cinq ans sont désormais résolues de façon routinière, et certainement cinq maintenant cette affirmation sera toujours vraie. Cela est même vrai lorsque les algorithmes utilisés sont intraitables.

Des exercices

1. Donnez une estimation de grand O pour le nombre d'opérations (lorsqu'une opération est un ajout ou une multiplication) utilisé dans ce segment d'un algorithme.

$t := 0$
pour $i := 1$ **à** 3
  pour $j := 1$ **à** 4
    $t := t + ij$

2. Donnez une estimation de grand O pour le nombre d'additions ce segment d'un algorithme.

$t := 0$
pour $i := 1$ **à** n
  pour $j := 1$ **à** n
    $t := t + i + j$

3. Donnez une estimation de grand O pour le nombre d'opérations, lorsqu'une opération est une comparaison ou une multiplication, utilisé dans ce segment d'un algorithme (en ignorant les isons utilisés pour tester les conditions dans les boucles **for** , où $a_1, a_2, \ldots, a_n$ sont des nombres réels positifs).

$m := 0$
pour $i := 1$ **à** n
  pour $j := i + 1$ **à** n
    $m := \max(a_i a_j, m)$

4. Donnez une estimation de grand O pour le nombre d'opérations, lorsqu'une opération est un ajout ou une multiplication, utilisée dans ce segment d'un algorithme (en ignorant les comparaisons utilisé pour tester les conditions dans le **temps** en boucle).

$i := 1$
$t := 0$
tandis que $i \leq n$
  $t := t + i$
  $i := 2i$

5. Combien de comparaisons sont utilisées par l'algorithme donné dans l'exercice 16 de la section 3.1 pour trouver le plus petit nombre dans une séquence de n nombres naturels?

6. a) Utilisez un pseudocode pour décrire l'algorithme qui place quatre premiers termes d'une liste de nombres réels d'arbitraires longueur dans l'ordre croissant en utilisant le tri par insertion.

b) Montrer que cet algorithme a une complexité temporelle $O(1)$ dans en termes de nombre de comparaisons utilisées.

7. Supposons qu'un élément soit connu pour être parmi les premiers quatre éléments dans une liste de 32 éléments. Un lin- recherche d'oreille ou recherche binaire localiser cet élément plus rapidement?

8. Étant donné un nombre réel x et un entier positif k , déterminez le nombre de multiplications utilisées pour trouver x^{2^k} départ avec x et au carré successivement (pour trouver x^2, x^4 , etc. sur). Est-ce un moyen plus efficace de trouver x^{2^k} que par plusieurs multiplier x par lui-même le nombre approprié de fois?

9. Donnez une estimation de grand O pour le nombre de comparaisons utilisé par l'algorithme qui détermine le nombre de 1 dans une chaîne de bits en examinant chaque bit de la chaîne pour déterminer déterminer s'il s'agit d'un bit 1 (voir l'exercice 25 de la section 3.1).

∗ **10. a)** Montrer que cet algorithme détermine le nombre de 1 bits dans la chaîne de bits S :

nombre de bits de **procédure** (S : chaîne de bits)
compte $:= 0$
tandis que $S = 0$
  count $:=$ *count* $+ 1$
  $S := S \wedge (S - 1)$
return *count* { *count* est le nombre de 1 dans S }

Ici $S - 1$ est la chaîne de bits obtenue en changeant le 1 bit le plus à droite de S à 0 et tous les 0 bits à droite de ceci à 1s. [Rappelons que $S \wedge (S - 1)$ est le bit à bit *ET* de S et $S - 1$.]

b) Combien d'opérations *ET au niveau du* bit sont nécessaires pour trouver le nombre de 1 bits dans une chaîne S *en* utilisant l'algorithme en partie (a)?

11. a) Supposons que nous ayons n sous-ensembles $S_1, S_2, \ldots, S_n$ de l'ensemble $\{1, 2, \ldots, n\}$. Exprimer un algorithme de force brute qui dé- termines s'il existe une paire disjointe de ces sous- ensembles. [*Astuce:* l'algorithme doit parcourir le sous-ensembles; pour chaque sous-ensemble S_i , il doit ensuite parcourir tous les autres sous-ensembles; et pour chacun de ces autres sous-ensembles S_j , il doit parcourir tous les éléments k de S_i pour dé- détermine si k appartient aussi à S_j .]

b) Donnez une estimation de grand O pour le nombre de l'algorithme doit déterminer si un entier est en l'un des sous-ensembles.

12. Considérez l'algorithme suivant, qui prend en entrée un séquence de n entiers $a_1, a_2, \ldots, a_n$ et produit en sortie mettre une matrice $\mathbf{M} = \{m_{ij}\}$ où m_{ij} est le terme minimum dans la séquence d'entiers $a_i, a_{i+1}, \ldots, a_j$ pour $j \geq i$ et $m_{ij} = 0$ sinon.

initialiser **M** pour que $m_{ij} = a_i$ si $j \geq i$ et $m_{ij} = 0$ autrement
pour $i := 1$ **à** n
  pour $j := i + 1$ **à** n
    pour $k := i + 1$ **à** j
      $m_{ij} := \min(m_{ij}, a_k)$
return $\mathbf{M} = \{m_{ij}\}$ { m_{ij} est la durée minimale de $a_i, a_{i+1}, \ldots, a_j$ }

a) Montrer que cet algorithme utilise des comparaisons $O(n^3)$ pour calculer la matrice **M** .

b) Montrer que cet algorithme utilise des comparaisons (n^3) pour calculer la matrice **M** . En utilisant ce fait et la partie (a), conclure que les algorithmes utilisent des comparaisons (n^3) . [*Indice:* ne considérez que les cas où $i \leq n/4$ et $j \geq 3n/4$ dans les deux boucles externes de l'algorithme.]

13. L'algorithme conventionnel pour évaluer un polynôme $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ à $x = c$ peut être exprimé en pseudocode par

```
polynôme de procédure (c, a0, a1, ..., an : nombres réels)
    puissance := 1
    y := a0
    pour i := 1 à n
        puissance := puissance * c
        y := y + ai * puissance
    renvoie y { y = an c^n + an-1 c^(n-1) + ··· + a1 c + a0 }
```

où la valeur finale de y est la valeur du polynôme à $x = c$.

a) Évaluez $3x^2 + x + 1$ à $x = 2$ en passant par chaque étape de l'algorithme montrant les valeurs attribuées à chaque étape de l'affectation.

b) Combien de multiplications et d'additions exactement utilisé pour évaluer un polynôme de degré n à $x = c$? (Ne comptez pas les ajouts utilisés pour incrémenter la boucle variable.)

14. Il existe un algorithme plus efficace (en termes de nombre nombre de multiplications et d'additions utilisées) pour évaluer polynômes que l'algorithme conventionnel décrit dans l'exercice précédent. C'est ce qu'on appelle **la méthode de Horner** . Ce pseudocode montre comment utiliser cette méthode pour trouver le valeur de $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ à $x = c$.

```
procédure Horner (c, a0, a1, a2, ..., an : nombres réels )
    y := an
    pour i := 1 à n
        y := y * c + an-i
    renvoie y { y = an c^n + an-1 c^(n-1) + ··· + a1 c + a0 }
```

a) Évaluez $3x^2 + x + 1$ à $x = 2$ en passant par chaque étape de l'algorithme montrant les valeurs attribuées à chaque étape de l'affectation.

b) Combien de multiplications et d'additions exactement utilisé par cet algorithme pour évaluer un polynôme de degré n à $x = c$? (Ne comptez pas les ajouts utilisés pour incrémenter la variable de boucle.)

15. Quel est le plus grand n pour lequel on peut résoudre en un deuxième un problème en utilisant un algorithme qui nécessite $f(n)$ opérations de bits, où chaque opération de bits est effectuée en dix^{-9} secondes, avec ces fonctions $f(n)$?

a) $\log n$ **b)** n **c)** $n \log n$
d) n^2 **e)** 2^n **f)** $n!$

16. Quel est le plus grand n pour lequel on peut résoudre dans un jour en utilisant un algorithme qui nécessite des opérations $f(n)$ bits, où chaque opération de bit est effectuée en 10^{-11} secondes, avec ces fonctions $f(n)$?

a) $\log n$ **b)** $1000n$ **c)** n^2
d) $1000n^2$ **e)** n^3 **f)** 2^n
g) 2^{2n} **h)** 2^{2^n}

17. Quel est le plus grand n pour lequel on peut résoudre dans une minute en utilisant un algorithme qui nécessite un *fonctionnement en* bits $f(n)$ où chaque opération de bit est effectuée en dix^{-12} secondes, avec ces fonctions $f(n)$?

a) journal journal n **b)** $\log n$ **c)** $(\log n)^2$
d) $1000000n$ **e)** n^2 **f)** 2^n
g) 2^{n^2}

18. Combien de temps un algorithme prend-il pour résoudre un problème lem de taille n si cet algorithme utilise $2n^2 + 2^n$ opérations, nécessitant chacun 10^{-9} secondes, avec ces valeurs de n ?

a) 10 **b)** 20 **c)** 50 **d)** 100

19. Combien de temps un algorithme utilise-t-il 2^{50} opérations besoin si chaque opération prend autant de temps?

a) 10^{-6} s **b)** 10^{-9} s **c)** 10^{-12} s

20. Quel est l'effet du temps requis pour résoudre un problème lem lorsque vous doublez la taille de l'entrée de n à $2n$, en supposant que le nombre de millisecondes de l'algorithme utilise pour résoudre le problème avec la taille d'entrée n est chacun de ces une fonction? [Exprimez votre réponse sous la forme la plus simple soit comme rapport, soit comme différence. Votre réponse peut être fonction de n ou d'une constante.]

a) journal journal n **b)** $\log n$ **c)** $100n$
d) $n \log n$ **e)** n^2 **f)** n^3
g) 2^n

21. Quel est l'effet sur le temps requis pour résoudre un problème lorsque vous augmentez la taille de l'entrée de n à $n + 1$, en supposant que le nombre de millisecondes de l'algorithme utilise pour résoudre le problème avec la taille d'entrée n est chacun de ces une fonction? [Exprimez votre réponse sous la forme la plus simple soit comme rapport, soit comme différence. Votre réponse peut être fonction de n ou d'une constante.]

a) $\log n$ **b)** $100n$ **c)** n^2
d) n^3 **e)** 2^n **f)** 2^{n^2}
g) $n!$

22. Déterminer le moins de comparaisons ou le meilleur des cas performance,

a) nécessaire pour trouver le maximum d'une séquence de n integers, en utilisant l'algorithme 1 de la section 3.1.

b) utilisé pour localiser un élément dans une liste de n termes avec un recherche linéaire.

c) utilisé pour localiser un élément dans une liste de n termes à l'aide d'un recherche binaire.

23. Analyser la performance moyenne du cas du linéaire algorithme de recherche, si exactement la moitié du temps l'élément x est pas dans la liste et si x est dans la liste, il est tout aussi probable être dans n'importe quelle position.

24. Un algorithme est appelé **optimal** pour la solution d'un problème par rapport à une opération spécifiée s'il n'y a pas algorithme pour résoudre ce problème en utilisant moins tions.

a) Montrer que l'algorithme 1 de la section 3.1 est optimal algorithme par rapport au nombre de comparaisons d'entiers. [*Remarque:* Comparaisons utilisées pour la comptabilité ne sont pas concernés ici.]

b) L'algorithme de recherche linéaire est-il optimal par rapport à le nombre de comparaisons d'entiers (non compris comparaisons utilisées pour la comptabilité dans la boucle)?

25. Décrivez la complexité temporelle la plus défavorable, mesurée en termes de comparaisons, de l'algorithme de recherche ternaire décrit dans l'exercice 27 de la section 3.1.

26. Décrivez la complexité temporelle la plus défavorable, mesurée en termes de comparaison, de l'algorithme de recherche décrit dans l'exercice 28 de la section 3.1.

27. Analyser la complexité temporelle la plus défavorable de l'algorithme vous avez conçu dans l'exercice 29 de la section 3.1 pour localiser un mode dans une liste d'entiers non décroissants.

28. Analyser la complexité temporelle la plus défavorable de l'algorithme vous avez conçu dans l'exercice 30 de la section 3.1 pour localiser tous modes dans une liste d'entiers non décroissants.

29. Analyser la complexité temporelle la plus défavorable de l'algorithme vous avez conçu dans l'exercice 31 de la section 3.1 pour trouver le premier terme d'une séquence d'entiers égaux à certains précédents terme.

30. Analyser la complexité temporelle la plus défavorable de l'algorithme vous avez conçu dans l'exercice 32 de la section 3.1 pour trouver tous termes d'une séquence qui sont supérieurs à la somme de tous termes précédents.

31. Analyser la complexité temporelle la plus défavorable de l'algorithme vous avez conçu dans l'exercice 33 de la section 3.1 pour trouver le premier terme d'une séquence inférieur au précédent immédiatement terme.

32. Déterminer la complexité la plus défavorable en termes de parisons de l'algorithme de l'exercice 5 dans la section 3.1 pour déterminer toutes les valeurs qui se produisent plus d'une fois dans un liste triée d'entiers.

33. Déterminer la complexité la plus défavorable en termes de comparaison isons de l'algorithme de l'exercice 9 de la section 3.1 pour déterminer si une chaîne de n caractères est un palin-drôme.

34. Combien de comparaisons la sélection trie-t-elle (voir préambule de l'exercice 41 de la section 3.1) pour trier n articles? Utilisez votre réponse à donner une Big- O estimation de la complexité du tri de sélection en termes de nombre de comparaisons pour le tri par sélection.

35. Trouvez une estimation du grand O pour la pire des termes de nombre de comparaisons utilisées et le nombre de termes échangés par le type d'insertion binaire décrit dans le préambule de l'exercice 47 de la section 3.1.

36. Montrer que l'algorithme gourmand de changement pour n cents utilisant des quarts, des dix sous, des nickels et des sous a $O(n)$ complexité mesurée en termes de comparaisons nécessaires.

Les exercices 37 et 38 traitent du problème de la programmation la plupart des entretiens sont possibles compte tenu des heures de début et de fin de n entretiens.

37. Trouver la complexité d'un algorithme de force brute pour planifier les discussions en examinant tous les sous-ensembles possibles des pourparlers. [*Astuce:* utilisez le fait qu'un ensemble avec n éléments a 2^n sous-ensembles.]

38. Trouver la complexité de l'algorithme gourmand pour la programmation le plus de discussions en ajoutant à chaque étape la conversation avec le heure de fin la plus proche compatible avec celles déjà programmées (Algorithme 7 de la section 3.1). Supposons que les discussions sont pas déjà triés par heure de fin au plus tôt et supposons que la complexité temporelle la plus défavorable du tri est $O(n \log n)$.

39. Décrivez comment le nombre de comparaisons utilisées dans le pire des cas change lorsque ces algorithmes sont utilisés pour rechercher un élément d'une liste lorsque la taille de la liste double de n à $2n$, où n est un entier positif.

a) recherche linéaire **b)** recherche binaire

40. Décrivez comment le nombre de comparaisons utilisées dans le pire des cas change lorsque la taille de la liste à trier double de n à $2n$, où n est un entier positif lorsque ces algorithmes de tri sont utilisés.

a) tri des bulles **b)** tri par insertion

c) tri par sélection (décrit dans le préambule de cise 41 dans la section 3.1)

d) tri par insertion binaire (décrit dans le préambule de exercice 47 dans la section 3.1)

Une matrice $n \times n$ est appelée **triangulaire supérieure** si $a_{ij} = 0$ quand-jamais $i > j$.

41. À partir de la définition du produit matriciel, décrivez un algorithme en anglais pour calculer le produit de deux matrices triangulaires supérieures qui ignorent ces produits dans les calculs qui sont automatiquement égaux à zéro.

42. Donnez une description pseudocode de l'algorithme dans Exer-taille 41 pour multiplier deux matrices triangulaires supérieures.

43. Combien de multiplications d'entrées sont utilisées par les gorithme trouvé dans l'exercice 41 pour multiplier deux $n \times n$ matrices triangulaires supérieures?

Dans les exercices 44 à 45, supposez que le nombre de multiplications des entrées utilisées pour multiplier une $p \times q$ matrice et un q x r matrice est pqr .

44. Quel est le meilleur ordre pour former le produit **ABC** si **A** , **B** , et **C** sont des matrices de dimensions 3 × 9, 9 × 4, et 4 × 2, respectivement?

45. Quel est le meilleur ordre pour former le produit **ABCD** si **A** , **B** , **C** et **D** sont des matrices de dimensions 30 × 10, 10 × 40, 40 × 50 et 50 × 30, respectivement?.

∗ **46.** Dans cet exercice, nous abordons le problème de **la correspondance** des **chaînes**

ing .

a) Expliquez comment utiliser un algorithme de force brute pour trouver la première occurrence d'une chaîne donnée de m caractères, appelé la **cible** , dans une chaîne de n caractères, où $m \leq n$, appelé le **texte** . [*Astuce:* pensez en termes de recherche-faire correspondre le premier caractère de la cible et vérifier les caractères successifs pour une correspondance, et si ils ne correspondent pas tous, déplaçant l'emplacement de départ un caractère à droite.]

b) Exprimez votre algorithme en pseudocode.

c) Donnez une estimation du grand O pour le pire plexité de l'algorithme de force brute que vous avez décrit.

Termes et résultats clés

TERMES

algorithme: une séquence finie d'instructions précises pour former un calcul ou résoudre un problème
algorithme de recherche: le problème de la localisation d'un élément dans un liste
algorithme de recherche linéaire: une procédure de recherche ment par élément
algorithme de recherche binaire: une procédure pour rechercher un or- liste réduite en divisant successivement la liste en deux
tri: la réorganisation des éléments d'une liste en prescrit commande
$f(x)$ est $O(g(x))$: le fait que $|f(x)| \leq C|g(x)|$ pour tout $x > k$ pour certaines constantes C et k
témoin de la relation $f(x)$ est $O(g(x))$: une paire C et k tel que $|f(x)| \leq C|g(x)|$ chaque fois que $x > k$
$f(x)$ est $(g(x))$: le fait que $|f(x)| \geq C|g(x)|$ pour tout $x > k$ pour certaines constantes positives C et k
$f(x)$ est $(g(x))$: le fait que $f(x)$ soit à la fois $O(g(x))$ et $(g(x))$
complexité temporelle: la durée nécessaire à un algorithme résoudre un problème
complexité de l'espace: la quantité d'espace dans la mémoire de l'ordinateur requis pour qu'un algorithme résout un problème
dans le pire des cas, la complexité du temps: la plus grande requis pour un algorithme pour résoudre un problème d'une taille donnée
complexité temporelle moyenne **:** la durée moyenne nécessaire à un algorithme pour résoudre un problème d'une taille donnée
paradigme algorithmique: une approche générale de la construction algorithmes basés sur un concept particulier
force brute: le paradigme algorithmique basé sur la construction algorithmes pour résoudre les problèmes de manière naïve à partir de la énoncé du problème et définitions
algorithme gourmand: un algorithme qui fait le meilleur choix à chaque étape selon une condition spécifiée
problème traitable: un problème pour lequel il y a le pire des cas algorithme en temps polynomial qui le résout
problème insoluble: un problème pour lequel aucun pire cas il existe un algorithme polynomial pour le résoudre
problème résoluble: un problème qui peut être résolu par un rithm
problème insoluble: un problème qui ne peut pas être résolu par un algorithme

RÉSULTATS

algorithmes de recherche linéaire et binaire: (donnés dans la section 3.1)
tri à bulles: un tri qui utilise des passes où les éléments successifs sont échangés s'ils sont dans le mauvais ordre
tri par insertion: tri qui à la j ème étape insère le j ème élément dans la bonne position dans la liste, lorsque le premier $j - 1$ éléments de la liste sont déjà triés

La recherche linéaire a la complexité temporelle du pire des cas $O(n)$.
La recherche binaire a la complexité temporelle du pire des cas $O(\log n)$.
Les types de bulles et d'insertions ont $O(n^2)$ *le* pire des cas complexité.
$\log n!$ est $O(n \log n)$.
Si $f_1(x)$ est $O(g_1(x))$ et $f_2(x)$ est $O(g_2(x))$, alors $(f_1 + f_2)(x)$ est $O(\max(g_1(x), g_2(x)))$ et $(f_1 f_2)(x)$ est $O((g_1 g_2(x))$.
Si $a_0, a_1, \ldots, a_n$ sont des nombres réels avec $a_n = 0$, alors $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ est (x^n), et donc $O(n)$ et (n).

Questions de révision

1. a) Définissez le terme *algorithme* .

b) Quelles sont les différentes façons de décrire les algorithmes?

c) Quelle est la différence entre un algorithme de solvabilité un problème et un programme informatique qui résout ce problème?

2. a) Décrire, en anglais, un algorithme pour trouver le plus grand entier dans une liste de n entiers.

b) Exprimez cet algorithme en pseudocode.

c) Combien de comparaisons l'algorithme utilise-t-il?

3. a) Donner la définition du fait que $f(n)$ est $O(g(n))$, où $f(n)$ et $g(n)$ sont des fonctions de l'ensemble de entiers positifs à l'ensemble des nombres réels.

b) Utilisez la définition du fait que $f(n)$ est $O(g(n))$ directement pour prouver ou réfuter que $n^2 + 18n + 107$ est $O(n^3)$.

c) Utiliser la définition du fait que $f(n)$ est $O(g(n))$ directement pour prouver ou infirmer que n^3 est $O(n^2 + 18n + 107)$.

4. Énumérez ces fonctions de sorte que chaque fonction soit grande - O de la fonction suivante dans la liste: $(\log n)^3$, $n^3/1000000$ n, $100n + 101$, 3^n, $n!$, $2^n n^2$.

5. a) Comment pouvez-vous produire une estimation Big O pour une fonction c'est la somme des différents termes où chaque terme est le produit de plusieurs fonctions?

b) Donner une estimation de grand O pour la fonction $f(n) = (n! + 1)(2^n + 1) + (n^{n-2} + 8n^{n-3})(n^3 + 2^n)$. Pour la fonction g dans votre estimation $f(x)$ est $O(g(x))$ utilisez un fonction simple du plus petit ordre possible.

6. a) Définissez quelle est la complexité temporelle la plus défavorable, complexité temporelle des cas et complexité temporelle optimale (en termes de comparaisons) signifie pour un algorithme qui trouve le plus petit entier dans une liste de n entiers.

b) Quels sont les cas les plus défavorables, les cas moyens et les meilleurs cas complexités temporelles, en termes de comparaisons, des gorithme qui trouve le plus petit entier dans une liste de n entiers en comparant chacun des entiers avec le le plus petit entier trouvé jusqu'à présent?

7. a) Décrire l'algorithme de recherche linéaire et de recherche binaire

b) Utilisez l'algorithme de tri par insertion pour trier la liste 2, 5, 1, pour trouver un entier dans une liste d'entiers en augmentation commande.

b) Comparer les complexités temporelles les plus défavorables de ces deux algorithmes.

c) L'un de ces algorithmes est-il toujours plus rapide que l'autre (mesuré en termes de comparaisons)?

8. a) Décrivez l'algorithme de tri des bulles.

b) Utilisez l'algorithme de tri à bulles pour trier la liste 5, 2, 4, 1, 3.

c) Donnez une estimation de grand *O* pour le nombre de comparaisons utilisé par le tri à bulles.

9. a) Décrivez l'algorithme de tri par insertion.

b) Utilisez l'algorithme de tri par insertion pour trier la liste 5, 2, 4, 3.

c) Donnez une estimation de grand *O* pour le nombre de comparaisons utilisé par le tri par insertion.

10. a) Expliquez le concept d'un algorithme gourmand.

b) Fournir un exemple d'algorithme gourmand qui fournit produit une solution optimale et explique pourquoi elle produit une solution optimale.

c) Fournir un exemple d'algorithme gourmand qui ne pas toujours produire une solution optimale et expliquer pourquoi il ne le fait pas.

11. Définissez ce que signifie qu'un problème peut être traité et ce que signifie qu'un problème peut être résolu.

Exercices supplémentaires

1. a) Décrire un algorithme pour localiser la dernière occurrence du plus grand nombre dans une liste d'entiers.

b) Estimez le nombre de comparaisons utilisées.

2. a) Décrire un algorithme pour trouver le premier et le deuxième les plus grands éléments d'une liste d'entiers.

b) Estimez le nombre de comparaisons utilisées.

3. a) Donnez un algorithme pour déterminer si une chaîne de bits contient une paire de zéros consécutifs.

b) Combien de comparaisons l'algorithme utilise-t-il?

4. a) Supposons qu'une liste contienne des nombres entiers du plus grand au plus petit et un nombre entier peut apparaître edly dans cette liste. Concevoir un algorithme qui localise tout occurrences d'un entier *x* dans la liste.

b) Estimez le nombre de comparaisons utilisées.

5. a) Adapter l'algorithme 1 de la section 3.1 pour trouver le maximum maman et le minimum d'une séquence de *n* éléments en employant un maximum temporaire et un temporaire minimum qui est mis à jour comme chaque élément successif est examiné.

b) Décrivez l'algorithme de la partie (a) en pseudocode.

c) Combien de comparaisons d'éléments dans la séquence sont effectués par cet algorithme? (Ne comptez pas parisons utilisés pour déterminer si la fin de la a été atteinte.)

6. a) Décrivez en détail (et en anglais) les étapes d'une gorithme qui trouve le maximum et le minimum d'un séquence de *n* éléments en examinant des paires de éléments successifs, en gardant une trace d'une maman et un minimum temporaire. Si *n* est impair, les deux maximum temporaire et minimum temporaire initialement égal au premier terme, et si *n* est pair, la température minimum et maximum temporaire doivent être trouvé en comparant les deux éléments initiaux. Le tem- le maximum provisoire et le minimum temporaire mis à jour en les comparant avec le maximum et minimum de la paire d'éléments examinés.

b) Exprimer l'algorithme décrit dans la partie (a) en pseu- docode.

c) Combien de comparaisons d'éléments de la séquence sont effectués par cet algorithme? (Ne comptez pas parisons utilisés pour déterminer si la fin de la a été atteinte.) Comment cela se compare-t-il à le nombre de comparaisons utilisées par l'algorithme dans Exercice 5?

∗ **7.** Montrer que la complexité du pire des cas en termes de isons d'un algorithme qui trouve le maximum et le minimum la quantité de *n* éléments est au moins $\lceil 3n/2 \rceil - 2$.

8. Concevoir un algorithme efficace pour trouver le second le plus grand élément dans une séquence de *n* éléments et exploitez la complexité la plus défavorable de votre algorithme.

9. Concevez un algorithme qui trouve toutes les paires égales de sommes de deux termes d'une séquence de *n* nombres, et déterminer la pire complexité de votre algorithme.

10. Concevez un algorithme qui trouve la paire d'entiers la plus proche dans une séquence de *n* entiers, et déterminer le pire des cas complexité de votre algorithme. [*Astuce:* Triez la séquence. Utilisez le fait que le tri peut être effectué avec le pire des cas complexité $O(n \log n)$.]

Le **tri shaker** (ou **tri bulle bidirectionnel**) successivement compare des paires d'éléments adjacents, en les échangeant s'ils sont hors service, et en passant alternativement à travers la liste de du début à la fin puis de la fin au début jusqu'à ce qu'aucun échange ne soit nécessaire.

11. Affichez les étapes utilisées par le tri du shaker pour trier la liste 3, 5, 1, 4, 6, 2.

12. Exprimez le tri du shaker en pseudocode.

13. Montrer que le tri du shaker a une complexité $O(n^2)$ mesurée en termes de nombre de comparaisons qu'il utilise.

14. Expliquez pourquoi le tri par shaker est efficace pour le tri des listes qui sont déjà dans le bon ordre.

15. Montrer que $(n \log n + n^2)^3$ est $O(n^6)$.

16. Montrez que $8x^3 + 12x + 100 \log x$ est $O(x^3)$.

17. Donnez une estimation de grand *O* pour $(x^2 + x(\log x)^3) \cdot (2^x + x^3)$.

18. Trouvez une estimation du grand *O* pour $\sum_{j=1}^{n} j(j+1)$.

∗ **19.** Montrez que $n!$ n'est pas $O(2^n)$.

∗ **20.** Montrez que n^n n'est pas $O(n!)$.

21. Trouvez toutes les paires de fonctions du même ordre dans ce liste des fonctions: $n^2 + (\log n)^2$, $n^2 + n$, $n^2 + \log 2^n + 1$, $(n+1)^3 - (n-1)^3$, et $(n + \log n)^2$.

22. Trouvez toutes les paires de fonctions du même ordre dans cette liste de fonctions $n^2 + 2^n$, $n^2 + 2^{100}$, $n^2 + 2^{2n}$, $n^2 + n!$, $n^2 + 3^n$, et $(n^2 + 1)^2$.

23. Trouver un entier *n* avec $n > 2$ pour lequel $n^{2^{100}} < 2^n$.

24. Trouver un entier *n* avec $n > 2$ pour lequel $(\log n)^{2^{100}} < \sqrt{n}$.

∗ **25.** Organiser les fonctions $\sqrt{n}$, $(\log n)^2$, $n^{1.0001}$, $(1.0001)^n$, $2^{\log_2 n}$ et $n(\log n)^{1001}$ dans une liste de sorte que chaque fonction est grand - *O* de la fonction suivante. [*Astuce:* pour déterminer le taille relative de certaines de ces fonctions, prenez des logarithmes.]

∗ **26.** Organiser la fonction 2^{100n}, 2^{n^2}, $2^{n!}$, 2^{2^n}, $n^{\log n}$, $n \log n \log \log n$, $n^{3/2}$, $n(\log n)^{3/2}$, et $n^{\text{quatre/trois}}(\log n)^2$ dans un

31. Trouvez tous les partenaires valides pour chaque homme et chaque femme si il y a trois hommes m_1, m_2 et m_3 et trois femmes w_1, w_2, w_3 avec ces classements de préférence des hommes pour la femmes, du plus haut au plus bas: $m_1 : w_3, w_1, w_2$; $m_2 : w_3, w_2, w_1$; $m_3 : w_2, w_3, w_1$; et avec ces préférences rang- des femmes pour les hommes, du plus haut au plus bas: $w_1 : m_3, m_2, m_1$; $w_2 : m_1, m_3, m_2$; $w_3 : m_3, m_2, m_1$.

∗ **32.** Montrer que l'algorithme d'acceptation différée donné dans le préambule de l'exercice 61 de la section 3.1, produit toujours un appariement pessimal masculin optimal et femelle.

33. Définir ce que cela signifie pour une correspondance d'être une femme optimale et pour qu'un appariement soit masculin pessimal.

∗ **34.** Montrez que lorsque la femme fait la proposition dans le différé algorithme d'acceptation, l'appariement produit est féminin optimal et mâle pessimal.

Dans les exercices 35 et 36, nous considérons les variations du problème liste de sorte que chaque fonction soit grande - O de la fonction suivante. [*Astuce:* Pour déterminer la taille relative de certains de ces fonctions, prenez des logarithmes.]

∗ 27. Donner un exemple de deux fonctions croissantes $f(n)$ et $g(n)$ de l'ensemble des entiers positifs à l'ensemble des posi- nombres entiers tels que ni $f(n)$ n'est $O(g(n))$ ni $g(n)$ est $O(f(n))$.

28. Montrer que si les dénominations des pièces sont $c^0, c^1, \ldots, c^k$, où k est un entier positif et c est un entier positif, $c > 1$, l'algorithme gourmand produit toujours des changements avec le moins de pièces possible.

29. a) Utilisez un pseudocode pour spécifier un algorithme de force brute qui détermine le moment donné en entrée une séquence de n pos- entiers itifs s'il y a deux termes distincts de la séquence qui a pour somme un troisième terme. L'algo- rithm devrait parcourir tous les triplets de termes de la séquence, vérifier si la somme des deux premiers termes est égal au troisième.

b) Donner un Big- O estimation de la complexité de le brutal forcer l'algorithme de la partie (a).

30. a) Concevoir un algorithme plus efficace pour résoudre le problème décrit l'exercice 29 qui trie d'abord les informations mettre la séquence, puis vérifie pour chaque paire de termes si leur différence est dans la séquence.

b) donner une Big- O estimer la complexité de cette al gorithme. Est-il plus efficace que l'algorithme de force brute? rithme de l'exercice 29?

Supposons que nous ayons s hommes et s femmes chacun avec leur préfé- listes de référence pour les membres du sexe opposé, comme décrit dans le préambule de l'exercice 60 de la section 3.1. Nous disons qu'un la femme w est un **partenaire valable** pour un homme m s'il y a des correspondant dans lequel ils sont appariés. De même, un homme m est un **partenaire valide** pour une femme w s'il y a une correspondance stable dans lequel ils sont appariés. Une correspondance dans laquelle chaque homme est a signé son partenaire valide se classant au premier rang de sa liste de préférences est appelé **mâle optimal** , et une correspondance dans laquelle chaque femme se voit attribuer son partenaire valide au rang le plus bas selon sa préférence la liste est appelée **femelle pessimale** .

de trouver des appariements stables d'hommes et de femmes décrits dans le préambule de l'exercice 61 de la section 3.1.

∗ 35. Dans cet exercice, nous considérons les problèmes d'appariement où il peut y avoir différents nombres d'hommes et de femmes, donc qu'il est impossible de faire correspondre tout le monde avec un membre de le sexe opposé.

a) Étendre la définition d'une correspondance stable à partir de celle donnée dans le préambule de l'exercice 60 de la section 3.1 pour couvrir le cas où il y a un nombre inégal de hommes et femmes. Évitez tous les cas où un homme et un les femmes se préféreraient mutuellement à leur y compris celles impliquant des personnes sans égal. (Supposons qu'une personne sans égal préfère une correspondance avec un membre du sexe opposé au reste incomparable.)

b) Adapter l'algorithme d'acceptation différée pour trouver des statistiques appariements fiables, en utilisant la définition d'appariements stables de la partie (a), quand il y a un nombre différent d'hommes et les femmes.

c) Démontrer que toutes les correspondances produites par l'algorithme de la partie (b) sont stables, selon la définition de la partie (a).

∗ 36. Dans cet exercice, nous considérons les problèmes d'appariement où certaines paires homme-femme ne sont pas autorisées.

a) Étendre la définition d'un appariement stable pour couvrir la situation où il y a le même nombre d'hommes femmes, mais certaines paires d'hommes et de femmes sont interdit. Évitez tous les cas où un homme et une femme se préféreraient mutuellement à leur situation actuelle, y compris ceux impliquant des personnes sans égal.

b) Adapter l'algorithme d'acceptation différée pour trouver stable appariements quand il y a le même nombre d'hommes femmes, mais certaines paires homme-femme sont interdites tanière. Assurez-vous de prendre en compte les personnes sans égal la fin de l'algorithme. (Supposons qu'un inégalé la personne préfère un match avec un membre de l'opposé sexe qui n'est pas un partenaire interdit de rester incomparable.)

c) Démontrer que toutes les correspondances produites par l'algorithme de (b) sont stables, selon la définition en partie (une).

Les exercices 37 à 40 traitent du problème de la planification de n travaux sur un seul processeur. Pour terminer le travail j , le processeur doit exécuter travail j pour le temps t_j sans interruption. Chaque emploi a un mort- ligne d_j . Si nous commençons le travail j à l'instant s_j , il sera terminé à temps $e_j = s_j + t_j$. Le **retard** de l'emploi mesure la durée il se termine après son échéance, c'est-à-dire que le retard du travail j est $\max(0, e_j - d_j)$. Nous souhaitons concevoir un algorithme gourmand qui minimise le retard maximum d'un travail parmi les n travaux.

37. Supposons que nous ayons cinq emplois avec des délais requis spécifiés et délais: $t_1 = 25$, $d_1 = 50$; $t_2 = 15$, $d_2 = 60$; $t_3 = 20$, $d_3 = 60$; $t_4 = 5$, $d_4 = 55$; $t_5 = 10$, $d_5 = 75$. Trouvez le retard maximal de tout travail lorsque les travaux sont planifiés dans cet ordre (et ils commencent à l'instant 0): Job 3, Job 1, Job 4, Job 2, Job 5. Répondez à la même question pour l'horaire Travail 5, Travail 4, Travail 3, Travail 1, Travail 2.

38. La **faiblesse** d'un emploi nécessitant un temps t et avec un délai d est $d - t$, la différence entre son échéance et le temps qu'il faut. Trouvez un exemple qui montre que emplois en augmentant le relâchement ne donne pas toujours une calendrier avec le plus petit retard possible possible.

39. Trouvez un exemple qui montre que la planification des travaux dans du temps croissant nécessaire ne donne pas toujours une calendrier avec le plus petit retard possible possible.

∗ 40. Prouver que la planification des travaux par ordre de délais croissants produit toujours un programme qui minimise le maximum retard d'un travail. [*Astuce:* montrer d'abord que pour un calendrier à être optimal, les travaux doivent être planifiés sans interruption entre eux et pour qu'aucun travail ne soit planifié avant un autre avec une date limite antérieure.]

41. Supposons que nous ayons un sac à dos d'une capacité totale de

sac de couchage, une tente de 8 kg, un emballage alimentaire de 7 kg, un 4 kg contenant d'eau et un réchaud portatif de 11 kg.

Dans les exercices 42 à 46, nous étudierons le problème de l'équilibrage de charge ing. L'entrée au problème est une collection de processeurs p et n travaux, t_j est le temps nécessaire pour exécuter le travail j , les travaux exécutés sans interruption sur une seule machine jusqu'à la fin, et un processus sor ne peut exécuter qu'un seul travail à la fois. La **charge** L_k du processeur k est la somme de toutes les tâches affectées au processeur k des temps requis pour exécuter ces travaux. Le **makespan** est le maximum charge sur tous les processeurs p . Le problème de l'équilibrage de charge demande une affectation de tâches aux transformateurs afin de makespan.

42. Supposons que nous ayons trois processeurs et cinq emplois nécessitant fois $t_1 = 3$, $t_2 = 5$, $t_3 = 4$, $t_4 = 7$ et $t_5 = 8$. Résoudre le problème d'équilibrage de charge pour cette entrée en trouvant le affectation des cinq tâches aux trois processeurs minimise le makespan.

43. Supposons que L^* est le makespan minimum lorsque p pro- les cesseurs reçoivent n emplois, où t_j est le temps nécessaire pour exécuter le travail j .

a) Montrer que $L^* \geq \max_{j=1,2,\ldots,n} t_j$.

b) Montrer que $L^* \geq \frac{1}{p} \sum_{j=1}^{n} t_j$.

44. Ecrivez en pseudocode l'algorithme gourmand qui va à travers les emplois dans l'ordre et attribue chaque emploi au programme cessor avec la plus petite charge à ce point dans l'algorithme.

45. Exécutez l'algorithme de l'exercice 44 sur l'entrée donnée dans Exercice 42.

Un **algorithme d'approximation** pour un problème d'optimisation produit une solution garantie proche d'une solution optimale lution. Plus précisément, supposons que le problème d'optimisation demande une entrée S qui minimise $F(X)$ où F est un peu

W kg. Nous avons également n éléments où l'élément j a une masse w_j. Le **problème du sac à dos** demande un sous-ensemble de ces n éléments avec la plus grande masse totale ne dépassant pas possible W.

a) Concevoir un algorithme de force brute pour résoudre le problème problème de sac.

b) Résoudre le problème du sac à dos lorsque la capacité du sac à dos est de 18 kg et il y a cinq articles: un 5 kg

fonction de l'entrée X. Si un algorithme trouve toujours une entrée T avec $F(T) \leq cF(S)$ où c est un nombre réel positif fixe, l'algorithme est appelé un ***c*** **- algorithme d'approximation** pour la problème.

∗ **46.** Démontrer que l'algorithme de l'exercice 44 est un 2-algorithme d'approximation pour le problème d'équilibrage de charge. [*Astuce:* utilisez les deux parties de l'exercice 43.]

Projets informatiques

Écrivez des programmes avec ces entrées et sorties.

1. Étant donné une liste de n entiers, trouvez le plus grand entier dans le liste.

2. Étant donné une liste de n entiers, trouvez les première et dernière occurrences du plus grand entier de la liste.

3. Étant donné une liste de n entiers distincts, déterminez la position d'un entier dans la liste à l'aide d'une recherche linéaire.

4. Étant donné une liste ordonnée de n nombres entiers distincts, déterminez position d'un entier dans la liste à l'aide d'une recherche binaire.

5. Étant donné une liste de n nombres entiers, triez-les à l'aide d'un tri à bulles.

6. Étant donné une liste de n entiers, triez-les en utilisant une insertion Trier.

7. Étant donné un entier n, utilisez l'algorithme gourmand pour trouver le changer pour n cents en utilisant les quarts, les dix sous, les nickels et centimes.

8. Étant donné les heures de début et de fin de n entretiens, utilisez le algorithme gourmand approprié pour planifier le plus de discussions possible dans une seule salle de conférence.

9. Étant donné une liste ordonnée de n entiers et un entier x dans le liste, trouver le nombre de comparaisons utilisées pour déterminer la position de x dans la liste en utilisant une recherche linéaire et en utilisant une recherche binaire.

10. À partir d'une liste d'entiers, déterminez le nombre de isons utilisés par le tri à bulles et par le tri par insertion pour trier cette liste.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Nous savons que n^b est $O(d^n)$ lorsque b et d sont positifs nombres avec $d \geq 2$. Donner des valeurs des constantes C et k tel que $n^b \leq Cd^n$ chaque fois que $x > k$ pour chacun d'eux ensembles de valeurs: $b = 10$, $d = 2$; $b = 20$, $d = 3$; $b = 1000$, $d = 7$.

2. Calculez la variation pour différentes valeurs de n avec des pièces de différentes dénominations en utilisant l'algorithme gourmand et déterminer si le plus petit nombre de pièces était utilisé. Pouvez-vous trouver des conditions pour que l'algorithme gourmand est garanti d'utiliser le moins de pièces possible?

3. Utilisation d'un générateur d'ordonnances aléatoires des entiers 1 , 2 , ..., n , trouver le nombre de comparaisons utilisées par le tri à bulles, le tri par insertion, le tri par insertion binaire et selection sort pour trier ces entiers.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Examinez l'historique de l' *algorithme des* mots et décrivez l'utilisation de ce mot dans les premiers écrits.

2. Recherchez l'introduction originale de Bachmann de big- O notation. Expliquez comment lui et d'autres ont utilisé cette notation.

3. Expliquez comment les algorithmes de tri peuvent être classés en taxonomie basée sur le principe sous-jacent sur lequel ils sont basés.

4. Décrivez l'algorithme de tri radix.

5. Décrire les tendances historiques de la rapidité avec laquelle les transformateurs peuvent effectuer des opérations et utiliser ces tendances pour estimer rapidement les processeurs pourront effectuer des opérations les vingt prochaines années.

6. Élaborer une liste détaillée des paradigmes algorithmiques et des pro-présenter des exemples utilisant chacun de ces paradigmes.

7. Expliquez ce qu'est le prix Turing et décrivez les critères utilisé pour sélectionner les gagnants. Énumérez six anciens lauréats du prix et pourquoi ils ont reçu le prix.

8. Décrivez ce que l'on entend par algorithme parallèle. Explique comment le pseudocode utilisé dans ce livre peut être étendu à gérer des algorithmes parallèles.

9. Expliquez comment la complexité des algorithmes parallèles peut être mesuré. Donnez quelques exemples pour illustrer ce concept, montrant comment un algorithme parallèle peut fonctionner plus rapidement que celui qui ne fonctionne pas en parallèle.

10. Décrivez six problèmes NP-complets différents.

11. Démontrer comment l'un des nombreux NP-complet différents les problèmes peuvent être réduits au problème de satisfiabilité.

CHAPITRE

Théorie des nombres et cryptographie

La partie des mathématiques consacrée à l'étude de l'ensemble des entiers et de leurs propriétés est connue sous le nom de théorie des nombres. Dans ce chapitre, nous développerons certains des concepts importants de la théorie des nombres, y compris beaucoup de ceux utilisés en informatique. Au fur et à mesure que nous développons théorie, nous utiliserons les méthodes de preuve développées au chapitre 1 pour prouver de nombreux théorèmes.

Nous allons d'abord introduire la notion de divisibilité des entiers, que nous utilisons pour introduire modulaire, ou horloge, arithmétique. L'arithmétique modulaire fonctionne avec les restes d'entiers lorsqu'ils sont divisés par un entier positif fixe, appelé module. Nous en prouverons beaucoup des résultats importants sur l'arithmétique modulaire que nous utiliserons largement dans ce chapitre.

Les entiers peuvent être représentés avec n'importe quel entier positif b supérieur à 1 comme base. Dans ce chapitre, nous discutons des représentations de base b d'entiers et donnons un algorithme pour les trouver. En particulier, nous discuterons des représentations binaires, octales et hexadécimales (base 2, 8 et 16). Nous décrirons des algorithmes pour effectuer l'arithmétique à l'aide de ces représentations et étudierons leur complexité. Ces algorithmes ont été les premières procédures appelées algorithmes.

Nous allons discuter des nombres premiers, les entiers positifs qui n'ont que 1 et eux-mêmes comme diviseurs positifs. Nous prouverons qu'il existe une infinité de nombres premiers; la preuve que nous donnons est considérée comme l'une des plus belles preuves en mathématiques. Nous discuterons de la distribution des nombres premiers et de nombreuses questions ouvertes célèbres concernant les nombres premiers. Nous présenterons le concept de plus grands diviseurs communs et étudier l'algorithme euclidien pour les calculer. Cet algorithme a été décrite pour la première fois il y a des milliers d'années. Nous présenterons le théorème fondamental de arithmétique, un résultat clé qui nous dit que chaque entier positif a une factorisation unique en nombres premiers.

Nous expliquerons comment résoudre les congruences linéaires, ainsi que les systèmes de congruences linéaires, que nous résolvons en utilisant le célèbre théorème du reste chinois. Nous introduirons la notion de pseudoprimes, qui sont des entiers composites déguisés en nombres premiers, et montrent comment cette notion peut nous aider à générer rapidement des nombres premiers.

Ce chapitre présente plusieurs applications importantes de la théorie des nombres. En particulier, nous utilisera la théorie des nombres pour générer des nombres pseudo-aléatoires, pour attribuer des emplacements de mémoire à fichiers informatiques, et pour trouver les chiffres de contrôle utilisés pour détecter les erreurs dans divers types d'identification Nombres. Nous introduisons également le sujet de la cryptographie. La théorie des nombres joue essentiellement rôle à la fois dans la cryptographie classique, utilisée pour la première fois il y a des milliers d'années, et la cryptographie moderne, qui joue un rôle essentiel dans la communication électronique. Nous montrerons comment les idées que nous développer peut être utilisé dans des protocoles cryptographiques, introduisant des protocoles pour le partage de clés et pour l'envoi de messages signés. La théorie des nombres, autrefois considérée comme le plus pur des sujets, est devenue un outil essentiel pour assurer la sécurité informatique et Internet.

Divisibilité et arithmétique modulaire

introduction

Les idées que nous développerons dans cette section sont basées sur la notion de divisibilité. Division d'un entier par un entier positif produit un quotient et un reste. Travailler avec ces restes conduit à l'arithmétique modulaire, qui joue un rôle important en mathématiques et qui est utilisé tout au long de l'informatique. Nous discuterons quelques applications importantes de l'arithmétique modulaire plus loin dans ce chapitre, y compris la génération de nombres pseudo-aléatoires, l'attribution de mémoire à l'ordinateur des emplacements vers des fichiers, la construction de chiffres de contrôle et le cryptage des messages.

Division

Lorsqu'un entier est divisé par un deuxième entier non nul, le quotient peut ou non être un nombre entier. Par exemple, le $12 / 3 = 4$ est un nombre entier, alors que les onze $/ 4 = 2.75$ ne l'est pas. Cela mène à Définition 1.

DÉFINITION 1 Si a et b sont des entiers avec $a = 0$, on dit que *a divise b* s'il y a un entier c tel que $b = ac$, ou de manière équivalente, si $\frac{b}{une}$ est un entier. Quand a divise b, nous disons que a est un *facteur* ou un *diviseur* de b, et que b est un *multiple* de a. La notation $a \mid b$ signifie que a divise b. Nous écrivons *un* $\mid b$ quand a ne divise pas b.

Remarque: on peut exprimer *un* $\mid b$ *en* utilisant des quantificateurs comme $\exists c\ (ac = b)$, où l'univers du discours est l'ensemble des entiers.

Sur la figure 1, une ligne numérique indique quels entiers sont divisibles par l'entier positif d.

EXEMPLE 1 Déterminer si $3 \mid 7$ et si $3 \mid 12$.

Solution: nous voyons que $3 \mid 7$, parce que $7 / 3$ ne soit pas un nombre entier. En revanche, $3 \mid 12$ car Douze $/ 3 = 4$. ▲

EXEMPLE 2 Soit n et d des entiers positifs. Combien d'entiers positifs ne dépassant pas n sont divisibles par d ?

Solution: les entiers positifs divisibles par d sont tous les entiers de la forme dk, où k est un entier positif. Par conséquent, le nombre d'entiers positifs divisibles par d qui ne dépassent pas n est égal au nombre d'entiers k avec $0 < dk \leq n$, ou avec $0 < k \leq n / d$. Il existe donc $\lfloor n / d \rfloor$ entiers positifs ne dépassant pas n qui sont divisibles par d. ▲

Certaines des propriétés de base de la divisibilité des nombres entiers sont données dans le théorème 1.

THÉORÈME 1 Soit a, b et c *des* entiers, où $a = 0$. Alors

(*i*) si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$;
(*ii*) si *un* $\mid b$, alors $a \mid bc$ pour tous les entiers c ;
(*iii*) si *un* $\mid b$ et $b \mid c$, alors $a \mid c$.

Preuve: Nous fournirons une preuve directe de (*i*). Supposons que *un* $\mid b$ et $a \mid c$. Ensuite, à partir de la définition de divisibilité, il s'ensuit qu'il existe des entiers s et t avec $b = as$ et $c = at$. Par conséquent,

$$b + c = as + at = a(s + t).$$

$-3\,d$ $-2\,d$ $-\,d$ 0 *ré* $2\,j$ 3 *jours*

FIGURE 1 **Entiers divisibles par l'entier positif *d*.**

Par conséquent, a divise $b + c$. Cela établit la partie (i) du théorème. Les preuves des parties (ii) et (iii) sont laissés comme exercices 3 et 4.

Le théorème 1 a cette conséquence utile.

COROLLARY 1 Si a , b et c sont des entiers, où a = 0, tels que $a \mid b$ et $a \mid c$, alors $a \mid mb + nc$ chaque fois m et n sont des entiers.

Preuve: Nous donnerons une preuve directe. En partie (ii) du théorème 1 , nous voyons que *un* | mb et a | NC chaque fois que m et n sont des entiers. En partie (i) du théorème 1 , il en résulte que d' *un* | $mb + nc$.

L'algorithme de division

Lorsqu'un entier est divisé par un entier positif, il y a un quotient et un reste, comme algorithme de division montre.

THÉORÈME 2 **L'ALGORITHME DE DIVISION** Soit a un entier et d un entier positif. Alors là sont des entiers uniques q et r , avec $0 \leq r < d$, tels que $a = dq + r$.

Nous reportons la preuve de l'algorithme de division à la section 5.2.(Voir l'exemple 5 et Exercice 37.)

Remarque: le théorème 2 n'est pas vraiment un algorithme.(Pourquoi pas?) Néanmoins, nous utilisons son Nom.

DÉFINITION 2 Dans l'égalité donnée dans l'algorithme de division, d est appelé le *diviseur* , a est appelé le *dividende* , q est appelé le *quotient* , et r est appelé le *reste* . Cette notation est utilisée pour exprimer la quotient et reste:

$$q = a \textbf{ div } d, \; r = a \textbf{ mod } d.$$

Remarque: Notez quedeux *un* **div** d et *un* **mod** d pour une durée déterminée d sontfonctions sur l'ensemble des intégers. De plus, lorsque a est un entier et d est un entier positif, on a *un* **div** $d = \lfloor a / d \rfloor$ et *un* **mod** $d = a - d$. (Voir exercice 18.)

Les exemples 3 et 4 illustrent l'algorithme de division.

EXEMPLE 3 Quels sont le quotient et le reste lorsque 101 est divisé par 11?

Solution: nous avons

$$101 = 11 \cdot 9 + 2.$$

Par conséquent, le quotient lorsque 101 est divisé par 11 est 9 = 101 **div** 11, et le reste est 2 = 101 **mod** 11. ▲

EXEMPLE 4 Quels sont le quotient et le reste lorsque −11 est divisé par 3?

Solution: nous avons

$$-11 = 3(-4) + 1.$$

Par conséquent, le quotient lorsque −11 est divisé par 3 est −4 = −11 **div** 3, et le reste est 1 = −11 **mod** 3.

Notez que le reste ne peut pas être négatif. Par conséquent, le reste n'est *pas* -2, même bien que

$$-11 = 3(-3) - 2,$$

car $r = -2$ ne satisfait pas $0 \leq r < 3$. ▲

Notez que l'entier a est divisible par l'entier d si et seulement si le reste est nul quand a est divisé par d.

Remarque: Un langage de programmation peut avoir un, voire deux opérateurs pour l'arithmétique modulaire. métique, notée par mod (en BASIC, Maple, Mathematica, EXCEL et SQL),% (en C, C ++, Java, et Python), rem (en Ada et Lisp), ou autre chose. Soyez prudent lorsque vous les utilisez, car pour $a < 0$, certains de ces opérateurs renvoient $a - m\lceil a/m \rceil$ au lieu d'*un* **mod** $m = a - m\lfloor a/m \rfloor$ (comme montré dans l'exercice 18). De plus, contrairement à *un* **mod** m, certains de ces opérateurs sont définis lorsque $m < 0$, et même lorsque $m = 0$.

Arithmétique modulaire

Dans certaines situations, nous nous soucions uniquement du reste d'un entier lorsqu'il est divisé par certains entier positif spécifié. Par exemple, lorsque nous demandons quelle heure il sera (sur une horloge de 24 heures) 50 dans quelques heures, nous nous soucions uniquement du reste lorsque 50 plus l'heure actuelle est divisée par 24. Parce que nous ne sommes souvent intéressés que par les restes, nous avons des notations spéciales pour eux. Nous avons déjà introduit la notation a **mod** m pour représenter le reste quand un entier a est divisé par l'entier positif m. Nous introduisons maintenant une notation différente, mais liée, qui indique que deux entiers ont le même reste lorsqu'ils sont divisés par l'entier positif m.

DÉFINITION 3 Si a et b sont des entiers et m est un entier positif, alors a est *congru à b modulo m* si m divise $a - b$. Nous utilisons la notation $a \equiv b \pmod{m}$ pour indiquer que a est congru avec b modulo m. On dit que $a \equiv b \pmod{m}$ est une **congruence** et que m est son **module** (pluriel **modules**). Si a et b ne sont pas modulo m congrus , on écrit $a \equiv b \pmod{m}$.

Bien que les deux notations $a \equiv b \pmod{m}$ et a **mod** $m = b$ incluent «mod», elles représentent concepts fondamentalement différents. Le premier représente une relation sur l'ensemble des entiers, alors que le second représente une fonction. Cependant, la relation $a \equiv b \pmod{m}$ et la fonction **mod** m sont étroitement liés, comme décrit dans le théorème 3.

THÉORÈME 3 Soit a et b *des* entiers, et m soit un entier positif. Alors $a \equiv b \pmod{m}$ si et seulement si a **mod** $m = b$ **mod** m .

La preuve du Théorème 3 est laissée comme Exercices 15 et 16. Rappelons que a **mod** m et b **mod** m sont les restes lorsque a et b sont divisés par m , respectivement. Par conséquent, le théorème 3 dit également que $a \equiv b \pmod{m}$ si et seulement si a et b ont le même reste lorsqu'ils sont divisés par m .

EXEMPLE 5 Déterminer si 17 est congru à 5 modulo 6 et si 24 et 14 sont congruents modulo 6.

Solution: Parce que 6 divise 17 - 5 = 12, nous voyons que $17 \equiv 5 \pmod{6}$.Cependant, parce que 24 - 14 = 10 n'est pas divisible par 6, on voit que $24 \equiv 14 \pmod{6}$. ▲

Le grand mathématicien allemand Karl Friedrich Gauss a développé le concept de congruence à la fin du XVIIIe siècle. La notion de congruences a joué un rôle important rôle dans le développement de la théorie des nombres.

Le théorème 4 fournit un moyen utile de travailler avec des congruences.

THÉORÈME 4 Soit m un entier positif. Les entiers a et b sont modulo m congrus si et seulement s'il y a est un entier k tel que $a = b + km$.

Preuve: Si $a \equiv b \ (\bmod m)$, par la définition de la congruence (Définition 3), on sait que $m \mid (a - b)$. Cela signifie qu'il existe un entier k tel que $a - b = km$, de sorte que $a = b + km$.
Inversement, s'il existe un entier k tel que $a = b + km$, alors $km = a - b$. Par conséquent, m divise $a - b$, de sorte que $a \equiv b \ (\bmod m)$.

L'ensemble de tous les entiers congruents à un entier a modulo m est appelé la **classe de congruence** d' *un* modulo m . Dans le chapitre 9, nous montrerons qu'il existe m classes d'équivalence disjointes par paire modulo m et que l'union de ces classes d'équivalence est l'ensemble des entiers.

Le théorème 5 montre que les additions et les multiplications préservent les congruences.

KARL FRIEDRICH GAUSS (1777–1855) Karl Friedrich Gauss, le fils d'un maçon, était un enfant prodige. Il a démontré son potentiel à l'âge de 10 ans, quand il a rapidement résolu un problème assigné par un enseignant à garder la classe occupée. L'enseignant a demandé aux élèves de trouver la somme des 100 premiers entiers positifs. Gauss a réalisé que cette somme pourrait être trouvée en formant 50 paires, chacune avec la somme 101: $1 + 100$, $2 + 99$, ..., $50 + 51$. Cet éclat a attiré le parrainage de mécènes, y compris le duc Ferdinand de Brunswick, qui l'a fait Gauss peut fréquenter le Collège Caroline et l'Université de Göttingen. Alors qu'il était étudiant, il a inventé la méthode des moindres carrés, qui est utilisée pour estimer la valeur la plus probable d'une variable à partir d'expériences résultats. En 1796, Gauss fit une découverte fondamentale en géométrie, faisant avancer un sujet qui n'avait pas avancé depuis les temps anciens. Il a montré qu'un polygone régulier à 17 côtés pouvait être tracé à l'aide d'une règle et d'une boussole.

En 1799, Gauss a présenté la première preuve rigoureuse du théorème fondamental de l'algèbre, qui stipule qu'un polynôme de le degré n a exactement n racines (en comptant les multiplicités). Gauss a atteint une renommée mondiale lorsqu'il a calculé avec succès l'orbite de le premier astéroïde découvert, Ceres, en utilisant des données rares.

Gauss a été appelé le prince des mathématiques par ses mathématiciens contemporains. Bien que Gauss soit connu pour ses nombreux découvertes en géométrie, algèbre, analyse, astronomie et physique, il avait un intérêt particulier pour la théorie des nombres, qui peut être vu de sa déclaration "Les mathématiques sont la reine des sciences, et la théorie des nombres est la reine des mathématiques." Gauss a posé les bases de la théorie moderne des nombres avec la publication de son livre *Disquisitiones Arithmeticae* en 1801.

THÉORÈME 5 Soit m un entier positif. Si $a \equiv b \ (\bmod m)$ et $c \equiv d \ (\bmod m)$, alors

$$a + c \equiv b + d \ (\bmod m) \qquad \text{et} \qquad ac \equiv bd \ (\bmod m).$$

Preuve: Nous utilisons une preuve directe. Parce *que* $a \equiv b \ (\bmod m)$ et $c \equiv d \ (\bmod m)$, par le théorème 4 il sont des entiers s et t avec $b = a + sm$ et $d = c + tm$. Par conséquent,

$$b + d = (a + sm) + (c + tm) = (a + c) + m\ (s + t)$$

et

$$bd = (a + sm)\ (c + tm) = ac + m\ (\grave{a} + cs + stm).$$

Par conséquent,

$$a + c \equiv b + d \pmod{m} \qquad \text{et} \qquad ac \equiv bd \pmod{m}.$$

EXEMPLE 6 Parce que $7 \equiv 2 \pmod{5}$ et $11 \equiv 1 \pmod{5}$, il résulte du Théorème 5 que

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

et cela

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$

▲

Vous ne pouvez pas toujours diviser les deux côtés d'une congruence par le même numéro!

Nous devons être prudents en travaillant avec les congruences.Certaines propriétés que nous pouvons nous attendre à être vraies ne sont pas valides. Par exemple, si $ac \equiv bc \pmod{m}$, la congruence $a \equiv b \pmod{m}$ peut être fausse. De même, si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, la congruence $a^c \equiv b^d \pmod{m}$ peut être faux. (Voir l'exercice 37.)

Le corollaire 2 montre comment trouver les valeurs de la fonction **mod** m à la somme et au produit de deux entiers en utilisant les valeurs de cette fonction à chacun de ces entiers.Nous utiliserons ce résultat dans Section 5.4.

COROLLARY 2 Soit m un entier positif et a et b des entiers. alors

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

et

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m.$$

Preuve: Par les définitions de **mod** m et de congruence modulo m, nous savons que $a \equiv (a \textbf{ mod } m) \pmod{m}$ et $b \equiv (b \textbf{ mod } m) \pmod{m}$. Par conséquent, le théorème 5 nous dit que

$$a + b \equiv (a \textbf{ mod } m) + (b \textbf{ mod } m) \pmod{m}$$

et

$$ab \equiv (a \textbf{ mod } m)(b \textbf{ mod } m) \pmod{m}.$$

Les égalités dans ce corollaire découlent de ces deux dernières congruences du théorème 3.

Module arithmétique m

On peut définir des opérations arithmétiques sur $\mathbf{Z}_m$, l'ensemble des entiers non négatifs inférieurs à m, c'est-à-dire, l'ensemble $\{0, 1, ..., m - 1\}$. En particulier, nous définissons l'addition de ces entiers, notés $+_m$ par

$$a +_m b = (a + b) \textbf{ mod } m,$$

où l'addition sur le côté droit de cette équation est l'addition ordinaire d'entiers, et nous définissons la multiplication de ces entiers, notée $\cdot_m$ par

$$a \cdot_m b = (a \cdot b) \textbf{ mod } m,$$

où la multiplication sur le côté droit de cette équation est la multiplication ordinaire de entiers. Les opérations $+_m$ et $\cdot_m$ sont appelées modules d'addition et de multiplication m et lorsque nous utilisons ces opérations, on dit que nous faisons du **modulo** m **arithmétique** .

EXEMPLE 7 Utilisez la définition de l'addition et de la multiplication dans $\mathbf{Z}_m$ pour trouver $7 +_{11} 9$ et $7 \cdot_{11} 9$.

Solution: En utilisant la définition de l'addition modulo 11, nous constatons que

$$7 +_{11} 9 = (7 + 9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5,$$

et

$$7 \cdot_{11} 9 = (7 \cdot 9) \textbf{ mod } 11 = 63 \textbf{ mod } 11 = 8.$$

D'où $7 +_{11} 9 = 5$ et $7 \cdot_{11} 9 = 8$.

▲

Les opérations $+_m$ et $\cdot_m$ satisfont plusieurs des mêmes propriétés d'addition ordinaire et multiplication d'entiers. Ils satisfont notamment à ces propriétés:

Fermeture Si a et b appartiennent à $\mathbf{Z}_m$, alors $a +_m b$ et $a \cdot_m b$ appartiennent à $\mathbf{Z}_m$.

Associativité Si a , b et c appartiennent à $\mathbf{Z}_m$, alors $(a +_m b) +_m c = a +_m (b +_m c)$ et $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Commutativité Si a et b appartiennent à $\mathbf{Z}_m$, alors $a +_m b = b +_m a$ et $a \cdot_m b = b \cdot_m a$.

Éléments d'identité Les éléments 0 et 1 sont des éléments d'identité pour l'addition et la multiplication modulo m , respectivement. Autrement dit, si a appartient à $\mathbf{Z}_m$, alors $a +_m 0 = 0 +_m a = a$ et $a \cdot_m 1 = 1 \cdot_m a = a$.

Inverses additifs Si $a = 0$ appartient à $\mathbf{Z}_m$, alors $m - a$ est l'inverse additif d' *un* modulo m et 0 est son propre inverse additif. Soit $a +_m (m - a) = 0$ et $0 +_m 0 = 0$.

Distributivité Si a , b et c appartiennent à $\mathbf{Z}_m$, alors $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ et $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Ces propriétés découlent des propriétés que nous avons développées pour les congruences et les restes modulo m , avec les propriétés des entiers;nous laissons leurs preuves comme Exercices 42–44. Notez que nous avons répertorié la propriété que chaque élément de $\mathbf{Z}_m$ a un inverse additif, mais pas une propriété analogue pour les inverses multiplicatifs a été incluse. C'est parce que multiplicatif les inverses n'existent pas toujours modulo m . Par exemple, il n'y a pas d'inverse multiplicatif de 2 modulo 6, comme le lecteur peut le vérifier. Nous reviendrons sur la question de savoir quand un entier a un module inverse multiplicatif m plus loin dans ce chapitre.

Page 265

Remarque: Parce que $\mathbf{Z}_m$ avec les opérations d'addition et de multiplication modulo m satisfait les propriétés énumérées, $\mathbf{Z}_m$ avec addition modulaire, serait un **groupe commutatif** et $\mathbf{Z}_m$ avec ces deux opérations, on dit qu'il s'agit d'un **anneau commutatif** . Notez que l'ensemble des entiers avec addition et multiplication ordinaires forme également un anneau commutatif. Les groupes et les anneaux sont étudié dans des cours qui couvrent l'algèbre abstraite.

Remarque: dans l'exercice 30 et dans les sections suivantes, nous utiliserons les notations + et · pour $+_m$ et $\cdot_m$ sans l'indice m sur le symbole de l'opérateur chaque fois que nous travaillons avec $\mathbf{Z}_m$.

Des exercices

1. Est-ce que 17 divise chacun de ces nombres?
a) 68 **b)** 84 **c)** 357 **d)** 1001

2. Démontrez que si a est un entier autre que 0, alors
a) 1 divise a . **b)** a divise 0.

3. Prouvez que la partie (*ii*) du théorème 1 est vraie.

4. Prouvez que la partie (*iii*) du théorème 1 est vraie.

5. Montrez que si *un* $\mid b$ et $b \mid a$, où a et b sont des entiers, alors $a = b$ ou $a = - b$.

6. Montrez que si a , b , c et d sont des entiers, où $a = 0$, tels que *un* $\mid c$ et $b \mid d$, puis $ab \mid cd$.

7. Montrez que si a , b et c sont des entiers, où $a = 0$ et $c = 0$, tel que $ac \mid bc$, puis $a \mid b$.

8. Prouvez ou réfutez que si *un* $\mid bc$, où a, b et c sont pos-entiers itifs et $a = 0$, alors $a \mid b$ ou $a \mid c$.

9. Quels sont le quotient et le reste quand
a) 19 est divisé par 7?
b) −111 est divisé par 11?
c) 789 est divisé par 23?
d) 1001 est divisé par 13?
e) 0 est divisé par 19?
f) 3 est divisé par 5?
g) -1 est divisé par 3?
h) 4 est divisé par 1?

10. Quels sont le quotient et le reste quand
a) 44 est divisé par 8?
b) 777 est divisé par 21?
c) −123 est divisé par 19?
d) -1 est divisé par 23?
e) −2002 est divisé par 87?

13. Supposons que a et b sont des entiers, $a \equiv 4 \pmod{13}$, et $b \equiv 9 \pmod{13}$. Trouver l'entier c avec $0 \leq c \leq 12$ tel cette
a) $c \equiv 9a \pmod{13}$.
b) $c \equiv 11b \pmod{13}$.
c) $c \equiv a + b \pmod{13}$.
d) $c \equiv 2a + 3b \pmod{13}$.
e) $c \equiv a^2 + b^2 \pmod{13}$.
f) $c \equiv a^3 - b^3 \pmod{13}$.

14. Supposons que a et b sont des entiers, $a \equiv 11 \pmod{19}$, et $b \equiv 3 \pmod{19}$. Trouver l'entier c avec $0 \leq c \leq 18$ tel cette
a) $c \equiv 13a \pmod{19}$.
b) $c \equiv 8b \pmod{19}$.
c) $c \equiv a - b \pmod{19}$.
d) $c \equiv 7a + 3b \pmod{19}$.
e) $c \equiv 2a^2 + 3b^2 \pmod{19}$.
f) $c \equiv a^3 + 4b^3 \pmod{19}$.

15. Soit m un entier positif. Montrer que $a \equiv b \pmod{m}$ si a **mod** $m = b$ **mod** m .

16. Soit m un entier positif. Montrer que *un* **mod** $m =$ b **mod** m si $a \equiv b \pmod{m}$.

17. Montrer que si n et k sont des entiers positifs, alors $\lceil n / k \rceil = \lfloor (n - 1) / k \rfloor + 1$.

18. Montrer que si a est un entier et d est un entier supérieur à 1, puis le quotient et le reste der obtenu lorsque a est divisé par d sont $\lfloor a / d \rfloor$ et $a - d \lfloor a / d$ respectively, respectivement.

19. Trouver une formule pour l'entier avec la plus petite valeur absolue qui est congru à un entier a modulo m , où m est un entier positif.

f) 0 est divisé par 17?
g) 1.234.567 est divisé par 1001?
h) −100 est divisé par 101?

11. **À** quelle heure une horloge de 12 heures lit-elle

a) 80 heures après la lecture de 11h00?
b) 40 heures avant de lire 12:00?
c) 100 heures après la lecture de 6h00?

12. **À** quelle heure une horloge de 24 heures lit-elle

a) 100 heures après la lecture de 2h00?
b) 45 heures avant de lire 12:00?
c) 168 heures après la lecture de 19h00?

20. Évaluez ces quantités.

a) −17 **mod** 2 **b)** 144 **mod** 7
c) −101 **mod** 13 **d)** 199 **mod** 19

21. Évaluez ces quantités.

a) 13 **mod** 3 **b)** −97 **mod** 11
c) 155 **mod** 19 **d)** −221 **mod** 23

22. Trouvez *un* **div** *m* et *un* **mod** *m* lorsque

a) $a = -111$, $m = 99$.
b) $a = -9999$, $m = 101$.
c) $a = 10299$, $m = 999$.
d) $a = 123456$, $m = 1001$.

23. Trouvez *un* **div** *m* et *un* **mod** *m* lorsque

a) $a = 228$, $m = 119$.
b) $a = 9009$, $m = 223$.
c) $a = -10101$, $m = 333$.
d) $a = -765432$, $m = 38271$.

24. Trouver l'entier a tel que

a) $a \equiv 43 \pmod{23}$ et $-22 \leq a \leq 0$.
b) $a \equiv 17 \pmod{29}$ et $-14 \leq a \leq 14$.
c) $a \equiv -11 \pmod{21}$ et $90 \leq a \leq 110$.

25. Trouvez l'entier a tel que

a) $a \equiv -15 \pmod{27}$ et $-26 \leq a \leq 0$.
b) $a \equiv 24 \pmod{31}$ et $-15 \leq a \leq 15$.
c) $a \equiv 99 \pmod{41}$ et $100 \leq a \leq 140$.

26. Énumérez cinq entiers qui sont congrus à 4 modulo 12.

27. Liste tous les entiers entre − 100 et 100 qui sont congrus à −1 modulo 25.

28. Décidez si chacun de ces nombres entiers est conforme à 3 modulo 7.

a) 37 **b)** 66
c) −17 **d)** −67

29. Décidez si chacun de ces nombres entiers est conforme à 5 modulo 17.

a) 80 **b)** 103
c) −29 **d)** −122

30. Trouvez chacune de ces valeurs.

a) (177 **mod** 31 + 270 **mod** 31) **mod** 31
b) (177 **mod** 31 · 270 **mod** 31) **mod** 31

31. Trouvez chacune de ces valeurs.

a) (−133 **mod** 23 + 261 **mod** 23) **mod** 23
b) (457 **mod** 23 · 182 **mod** 23) **mod** 23

32. Trouvez chacune de ces valeurs.

a) (19^2 **mod** 41) **mod** 9
b) (32^3 **mod** 13)^2 **mod** 11
c) (7^3 **mod** 23)^2 **mod** 31
d) (21^2 **mod** 15)^3 **mod** 22

33. Trouvez chacune de ces valeurs.

a) (99^2 **mod** 32)^3 **mod** 15
b) (3^4 **mod** 17)^2 **mod** 11
c) (19^3 **mod** 23)^2 **mod** 31
d) (89^3 **mod** 79)^4 **mod** 26

34. Montrer que si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, où a, b, c, d et m sont des entiers avec $m \geq 2$, alors $a - c \equiv b - d \pmod{m}$.

35. Montrer que si $n \mid m$, où n et m sont des entiers supérieurs de 1, et si $a \equiv b \pmod{m}$, où a et b sont des entiers, alors $a \equiv b \pmod{n}$.

36. Montrer que si a, b, c et m sont des entiers tels que $m \geq 2$, $c > 0$, et $a \equiv b \pmod{m}$, puis $ac \equiv bc \pmod{mc}$.

37. Trouvez des contre-exemples pour chacune de ces déclarations congruences.

a) Si $ac \equiv bc \pmod{m}$, où a, b, c et m sont des entiers avec $m \geq 2$, puis $a \equiv b \pmod{m}$.
b) Si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, où a, b, c, d et m sont des entiers avec c et d positifs et $m \geq 2$, puis $a^c \equiv b^d \pmod{m}$.

38. Montrer que si n est un entier alors $n^2 \equiv 0$ ou $1 \pmod{4}$.

39. Utilisez l'exercice 38 pour montrer que si m est un entier positif de la forme $4k + 3$ pour un entier non négatif k, alors m n'est pas la somme des carrés de deux entiers.

40. Démontrer que si n est un entier positif impair, alors $n^2 \equiv 1 \pmod{8}$.

41. Montrer que si a, b, k et m sont des entiers tels que $k \geq 1$, $m \geq 2$, et $a \equiv b \pmod{m}$, puis $a^k \equiv b^k \pmod{m}$.

42. Montrer que $\mathbf{Z}_m$ avec l'addition modulo m, où $m \geq 2$ est un entier, satisfait la fermeture, associative et commu- propriétés indicatives, 0 est une identité additive, et pour non nul $a \in \mathbf{Z}_m$, $m - a$ est l'inverse d' *un* modulo m.

43. Montrer que $\mathbf{Z}_m$ avec le module de multiplication m, où $m \geq 2$ est un entier, satisfait la fermeture, associative et propriétés de commutativité, et 1 est une identification multiplicative tité.

44. Montrer que la propriété distributive de la multiplication sur l'addition vaut pour $\mathbf{Z}_m$, où $m \geq 2$ est un entier.

45. Écrivez les tables d'addition et de multiplication pour $\mathbf{Z}_5$ (où par addition et multiplication, nous entendons $+_5$ et $\cdot_5$).

46. Écrivez les tables d'addition et de multiplication pour $\mathbf{Z}_6$ (où par addition et multiplication, nous entendons $+_6$ et $\cdot_6$).

47. Déterminer si chacune des fonctions $f(a) = a$ **div** d et $g(a) = a$ **mod** d, où d est un entier positif fixe, de l'ensemble d'entiers à l'ensemble d'entiers, est un à un, et déterminer si chacune de ces fonctions est activée.

Représentations entières et algorithmes

introduction

Les entiers peuvent être exprimés en utilisant n'importe quel entier supérieur à un comme base, comme nous le montrerons dans cette section. Bien que nous utilisons couramment décimal (base 10), les représentations, binaires (base 2), les représentations octales (base 8) et hexadécimales (base 16) sont souvent utilisées, en particulier en informatique science. Étant donné une base b et un entier n, nous montrerons comment construire lareprésentation de la base b de cet entier. Nous expliquerons également comment convertir rapidement entre binaire et octal et entre notations binaires et hexadécimales.

Comme mentionné dans la section 3.1, le terme *algorithme* se référait à l'origine aux procédures former des opérations arithmétiques en utilisant les représentations décimales des nombres entiers. Ces algorithmes, adapté pour une utilisation avec des représentations binaires, sont la base de l'arithmétique informatique. Ils fournissent bonnes illustrations du concept d'un algorithme et de la complexité des algorithmes. Pour ces raisons, ils seront abordés dans cette section.

Nous introduirons également un algorithme pour trouver *un* **div** *d* et *un* **mod** *d* où *a* et *d* sont entiers avec $d > 1$. Enfin, nous décrirons un algorithme efficace d'exponentiation modulaire, qui est un algorithme particulièrement important pour la cryptographie, comme nous le verrons dans la section 4.6.

Représentations d'entiers

Dans la vie de tous les jours, nous utilisons la notation décimale pour exprimer des entiers. Par exemple, 965 est utilisé pour désigner $9 \cdot 10^2 + 6 \cdot 10 + 5$. Cependant, il est souvent pratique d'utiliser des bases autres que 10. En particulier, les ordinateurs utilisent généralement la notation binaire (avec 2 comme base) lors de l'exécution de l'arithmétique, et notation octale (base 8) ou hexadécimale (base 16) lors de l'expression de caractères, tels que chiffres. En fait, nous pouvons utiliser n'importe quel entier supérieur à 1 comme base lors de l'expression des entiers. Cette est énoncé dans le théorème 1.

THÉORÈME 1 Soit b un entier supérieur à 1. Alors si n est un entier positif, il peut être exprimé de façon unique sous la forme

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

où k est un entier non négatif, $a_0, a_1, \ldots, a_k$ sont des entiers non négatifs inférieurs à b, et $a_k = 0$.

Une preuve de ce théorème peut être construite en utilisant l'induction mathématique, une méthode de preuve qui est abordé à la section 5.1. Il peut également être trouvé dans [Ro10]. La représentation de n donnée dans Le théorème 1 est appelé l'**expansion de base *b* de *n***. L'expansion de base b de n est notée $(a_k a_{k-1} \ldots a_1 a_0)_b$. Par exemple, $(245)_8$ représente $2 \cdot 8^2 + 4 \cdot 8 + 5 = 165$. Typiquement, le sous-le script 10 est omis pour les extensions de base 10 d'entiers car la base 10, ou **les extensions décimales**, sont couramment utilisés pour représenter des entiers.

EXPANSIONS BINAIRES Choisir 2 comme base donne des **extensions binaires** d'entiers. Dans la notation binaire de chaque chiffre est soit un 0 soit un 1. En d'autres termes, l'expansion binaire d'un entier n'est qu'une chaîne de bits. Expansions binaires (et extensions associées qui sont des variantes de binaires expansions) sont utilisés par les ordinateurs pour représenter et faire de l'arithmétique avec des entiers.

EXEMPLE 1 Quelle est l'expansion décimale de l'entier qui a $(1\ 0101\ 1111)_2$ comme expansion binaire?

Solution: nous avons

$$\begin{aligned}(1\ 0101\ 1111)_2 &= 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 \\ &\quad + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351.\end{aligned}$$

▲

EXPANSIONS OCTALES ET HEXADÉCIMALES Parmi les bases les plus importantes la science informatique est la base 2, la base 8 et la base 16. Les extensions de la base 8 sont appelées extensions **octales** et les extensions de base 16 sont **des** extensions **hexadécimales**.

EXEMPLE 2 Quelle est l'expansion décimale du nombre à expansion octale $(7016)_8$?

Solution: L' utilisation de la définition d'une expansion de base b avec $b = 8$ nous indique que

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8 + 6 = 3598.$$

▲

Seize chiffres différents sont requis pour les extensions hexadécimales. Habituellement, l'hexadécimal les chiffres utilisés sont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F, où les lettres A à F représentent les chiffres correspondant aux nombres 10 à 15 (en notation décimale).

EXEMPLE 3 Quelle est l'expansion décimale du nombre à expansion hexadécimale $(2AE0B)_{16}$?

Solution: L' utilisation de la définition d'une expansion de base b avec $b = 16$ nous indique que

$$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = 175627.$$

▲

Chaque chiffre hexadécimal peut être représenté à l'aide de quatre bits.Par exemple, nous voyons que $(1110\ 0101)_2 = (E5)_{16}$ car $(1110)_2 = (E)_{16}$ et $(0101)_2 = (5)_{16}$. **Octets** , qui sont des bits les chaînes de longueur huit peuvent être représentées par deux chiffres hexadécimaux.

CONVERSION DE BASE Nous allons maintenant décrire un algorithme pour construire l'expansion de base b sion d'un entier n . Tout d'abord, divisez n par b pour obtenir un quotient et le reste, c'est-à-dire

$$n = bq_0 + a_0, \qquad 0 \leq a_0 < b.$$

Le reste, un_0 , est le chiffre le plus à droite dans l'expansion de base b de n . Ensuite, divisez q_0 par b à obtenir

$$q_0 = bq_1 + a_1, \qquad 0 \leq a_1 < b.$$

On voit que un_1 est le deuxième chiffre de la droite dans la base$b$ expansion de n . Continuez processus, divisant successivement les quotients par b , obtenant des chiffres de base b supplémentaires comme des restes. Ce processus se termine lorsque nous obtenons un quotient égal à zéro. Il produit le base b chiffres de n de droite à gauche.

EXEMPLE 4 Trouvez l'expansion octale de $(12345)_{10}$.

Solution: divisez d'abord 12345 par 8 pour obtenir

$$12345 = 8 \cdot 1543 + 1.$$

La division successive des quotients par 8 donne

$$\begin{aligned} 1543 &= 8 \cdot 192 + 7, \\ 192 &= 8 \cdot 24 + 0, \\ 24 &= 8 \cdot 3 + 0, \\ 3 &= 8{,}0 + 3. \end{aligned}$$

Les restes successifs que nous avons trouvés, 1, 7, 0, 0 et 3, sont les chiffres de droite à la gauche de 12345 en base 8. Par conséquent,

$$(12345)_{10} = (30071)_8.$$

▲

EXEMPLE 5 Trouvez l'expansion hexadécimale de $(177130)_{10}$.

Solution: divisez d'abord 177130 par 16 pour obtenir

$$177130 = 16 \cdot 11070 + 10.$$

La division successive des quotients par 16 donne

$$\begin{aligned}
11070 &= 16 \cdot 691 + 14, \\
691 &= 16{,}43 + 3, \\
43 &= 16 \cdot 2 + 11, \\
2 &= 16{,}0 + 2.
\end{aligned}$$

Les restes successifs que nous avons trouvés, 10, 14, 3, 11, 2, nous donnent les chiffres de droite à gauche de 177130 dans l'expansion hexadécimale (base 16) de $(177130)_{10}$. Il s'ensuit que

$$(177130)_{10} = (2B3EA)_{16}.$$

(Rappelons que les nombres entiers 10, 11 et 14 correspondent aux chiffres hexadécimaux A, B et E, respectivement.) ▲

EXEMPLE 6 Trouvez l'expansion binaire de $(241)_{10}$.

Solution: divisez d'abord 241 par 2 pour obtenir

$$241 = 2 \cdot 120 + 1.$$

La division successive des quotients par 2 donne

$$\begin{aligned}
120 &= 2{,}60 + 0, \\
60 &= 2 \cdot 30 + 0, \\
30 &= 2 \cdot 15 + 0, \\
15 &= 2, 7 + 1, \\
7 &= 2 \cdot 3 + 1, \\
3 &= 2 \cdot 1 + 1, \\
1 &= 2 \cdot 0 + 1.
\end{aligned}$$

Les restes successifs que nous avons trouvés, 1, 0, 0, 0, 1, 1, 1, 1, sont les chiffres de droite à gauche dans l'expansion binaire (base 2) de $(241)_{10}$. Par conséquent,

$$(241)_{10} = (1111\ 0001)_2.$$ ▲

Le pseudocode donné dans l'algorithme 1 trouve l'expansion de base b $(a_{k-1} \ldots a_1 a_0)_b$ du entier n.

TABLEAU 1 **Représentation hexadécimale, octale et binaire des nombres entiers de 0 à 15.**

Décimal	0	1	2	3	4	5	6	sept	8	9	dix	11	12	13	14	15
Hexadécimal	0	1	2	3	4	5	6	sept	8	9	UNE	B	C	ré	E	F
Octal	0	1	2	3	4	5	6	sept	dix	11	12	13	14	15	16	17
Binaire	0	1	dix	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

ALGORITHME 1 Construction de la base b Expansions.

expansion de la base b de la **procédure** (n, b : entiers positifs avec $b > 1$)
$q := n$
$k := 0$
tandis que $q = 0$
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ { $(a_{k-1} \ldots a_1 a_0)_b$ est l' expansion de base b de n }

Dans l'algorithme 1, q représente le quotient obtenu par divisions successives par b , en commençant par $q = n$. Les chiffres de l' expansion de la base b sont les restes de ces divisions et sont donnés par q **mod** b . L'algorithme se termine lorsqu'un quotient $q = 0$ est atteint.

Remarque: Notez que l'algorithme 1 peut être considéré comme un algorithme gourmand, comme les chiffres de base b sont prises aussi grandes que possible à chaque étape.

CONVERSION ENTRE LES EXPANSIONS BINAIRES, OCTALES ET HEXADÉCIMALES

La conversion entre les expansions binaires et octales et entre les expansions binaires et hexadécimales est extrêmement facile car chaque chiffre octal correspond à un bloc de trois chiffres binaires et chacun le chiffre hexadécimal correspond à un bloc de quatre chiffres binaires, avec ces correspondances montré dans le tableau 1 sans 0 initial montré. (Nous le laissons comme exercices 13-16 pour montrer que c'est le cas.) Cette conversion est illustrée dans l'exemple 7.

EXEMPLE 7 Trouver les extensions octales et hexadécimales de $(11\ 1110\ 1011\ 1100)_2$ et les extensions binaires de $(765)_8$ et $(A8D)_{16}$.

Solution: pour convertir $(11\ 1110\ 1011\ 1100)_2$ en notation octale, nous groupons les digi-son en blocs de trois, en ajoutant des zéros initiaux au début du bloc le plus à gauche si nécessaire. Ces blocs, de gauche à droite, sont 011, 111, 010, 111 et 100, correspondant à 3, 7, 2, 7, et 4, respectivement. Par conséquent, $(11\ 1110\ 1011\ 1100)_2 = (37274)_8$. Pour convertir $(11\ 1110\ 1011\ 1100)_2$ en notation hexadécimale, nous regroupons les chiffres binaires en blocs de quatre, en ajoutant l'initiale des zéros au début du bloc le plus à gauche si nécessaire. Ces blocs, de gauche à droite, sont 0011, 1110, 1011 et 1100, correspondant aux chiffres hexadécimaux 3, E, B et C, respectivement. Par conséquent, $(11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$.

Pour convertir $(765)_8$ en notation binaire, nous remplaçons chaque chiffre octal par un bloc de trois binaires chiffres. Ces blocs sont 111, 110 et 101. Par conséquent, $(765)_8 = (1\ 1111\ 0101)_2$. Pour convertir $(A8D)_{16}$ en notation binaire, nous remplaçons chaque chiffre hexadécimal par un bloc de quatre chiffres binaires. Celles-ci les blocs sont 1010, 1000 et 1101. Par conséquent, $(A8D)_{16} = (1010\ 1000\ 1101)_2$. ▲

Algorithmes pour les opérations entières

Les algorithmes pour effectuer des opérations avec des nombres entiers en utilisant leurs extensions binaires sont extrêmement important en arithmétique informatique. Nous décrirons des algorithmes pour l'addition et la multiplication de deux entiers exprimés en notation binaire. Nous analyserons également les complexité opérationnelle de ces algorithmes, en termes de nombre réel d'opérations binaires utilisées. Tout au long de cette discussion, supposons que les extensions binaires de a et b soient

$$a = (a_{n-1} a_{n-2} \ldots a_1 a_0)_2,\ b = (b_{n-1} b_{n-2} \ldots b_1 b_0)_2,$$

de sorte que a et b ont chacun n bits (en mettant des bits égaux à 0 au début de l'une de ces extensions si nécessaire).

Nous mesurerons la complexité des algorithmes pour l'arithmétique entière en termes de nombre de bits dans ces nombres.

ALGORITHME D'ADDITION Considérons le problème de l'ajout de deux entiers en notation binaire. Une procédure pour effectuer l'addition peut être basée sur la méthode habituelle pour ajouter des nombres avec crayon et papier. Cette méthode procède en ajoutant des paires de chiffres binaires avec des portées, quand ils se produisent, pour calculer la somme de deux entiers.Cette procédure va maintenant être spécifiée en détail.

Pour ajouter a et b , ajoutez d'abord leurs bits les plus à droite.Cela donne

$$a_0 + b_0 = c_0 \cdot 2 + s_0,$$

où s_0 est le bit le plus à droite dans l'expansion binaire de $a + b$ et c_0 est le **report** , qui est soit 0 ou 1. Ajoutez ensuite la paire de bits suivante et le report,

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1,$$

où s_1 est le bit suivant (à partir de la droite) dans l'expansion binaire de $a + b$, et c_1 est le report. Continuez ce processus, en ajoutant les bits correspondants dans les deux extensions binaires et le report, pour déterminer le bit suivant à partir de la droite dans l'expansion binaire de $a + b$. À la dernière étape, ajoutez a_{n-1}, b_{n-1} et c_{n-2} pour obtenir $c_{n-1} \cdot 2 + s_{n-1}$. Le bit de tête de la somme est $s_n = c_{n-1}$. Cette produit l'expansion binaire de la somme, à savoir, $a + b = (s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$.

EXEMPLE 8 Ajouter $a = (1110)_2$ et $b = (1011)_2$.

Solution: en suivant la procédure spécifiée dans l'algorithme, notez d'abord que

$$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1,$$

de sorte que $c_0 = 0$ et $s_0 = 1$. Ensuite, parce que

$$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0,$$

il s'ensuit que $c_1 = 1$ et $s_1 = 0$. Continuant,

$$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0,$$

de sorte que $c_2 = 1$ et $s_2 = 0$. Enfin, parce que

$$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1,$$

s'ensuit que $c_3 = 1$ et $s_3 = 1$. Cela signifie que $s_4 = c_3 = 1$. Par conséquent, $s = a + b = (1\,1001)_2$.
Cet ajout est illustré à la figure 1, où les portées sont affichées en bleu. ▲

```
 111
 1110
+1011
11001
```

FIGURE 1 **Ajout $(1110)_2$ et $(1011)_2$.**

L'algorithme d'ajout peut être décrit en utilisant le pseudocode comme suit.

ALGORITHME 2 Addition de nombres entiers.

```
add de procédure ( a, b : entiers positifs)
{les extensions binaires de a et b sont (a_{n−1} a_{n−2} ... a_1 a_0)_2
   et (b_{n−1} b_{n−2} ... b_1 b_0)_2 , respectivement}
c : = 0
pour j : = 0 à n - 1
      d : = ⌊ (a_j + b_j + c) /2⌋
      s_j : = a_j + b_j + c - 2 d
      c : = d
s_n : = c
return (s_0 , s_1 , ..., s_n ) {l'expansion binaire de la somme est (s_n s_{n−1} ... s_0)_2 }
```

Ensuite, le nombre d'ajouts de bits utilisés par l'algorithme 2 sera analysé.

EXEMPLE 9 Combien d'ajouts de bits sont nécessaires pour utiliser l'algorithme 2 pour ajouter deux entiers à n bits (ou moins) dans leurs représentations binaires?

Solution: Deux entiers sont ajoutés en ajoutant successivement des paires de bits et, quand cela se produit, un report. L'ajout de chaque paire de bits et le report nécessitent deux ajouts de bits. Ainsi, le nombre total de les ajouts de bits utilisés représentent moins de deux fois le nombre de bits dans l'extension. Par conséquent, le nombre des ajouts de bits utilisés par l'algorithme 2 pour ajouter deux entiers à n bits est $O(n)$. ▲

ALGORITHME DE MULTIPLICATION Ensuite, considérons la multiplication de deux entiers à n bits a et b. L'algorithme conventionnel (utilisé lors de la multiplication au crayon et au papier) fonctionne comme suit. En utilisant la loi distributive, nous voyons que

$$\begin{aligned} ab &= a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}) \\ &= a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1}). \end{aligned}$$

Nous pouvons calculer ab en utilisant cette équation. On note d'abord que $ab_j = a$ si $b_j = 1$ et $ab_j = 0$ si $b_j = 0$. Chaque fois que nous multiplions un terme par 2, nous déplaçons son expansion binaire d'une place vers la gauche et ajoutez un zéro à la fin de l'extension. Par conséquent, nous pouvons obtenir $(ab_j)2^j$ en **déplaçant** l'expansion binaire de ab_j j place vers la gauche, en ajoutant j zéro bit à la fin de ce binaire expansion. Enfin, on obtient ab en additionnant les n entiers $ab_j 2^j$, $j = 0, 1, 2, \ldots, n - 1$.

L'algorithme 3 affiche cette procédure de multiplication.

ALGORITHME 3 Multiplication des entiers.

multiplier la **procédure** (a, b : entiers positifs)
{les extensions binaires de a et b sont $(a_{n-1} a_{n-2} \ldots a_1 a_0)_2$
et $(b_{n-1} b_{n-2} \ldots b_1 b_0)_2$, respectivement}
pour $j := 0$ **à** $n - 1$
  si $b_j = 1$ **alors** $c_j := a$ décalé j lieux
  sinon $c_j := 0$
{ $c_0, c_1, \ldots, c_{n-1}$ sont les produits partiels}
$p := 0$
pour $j := 0$ **à** $n - 1$
  $p := p + c_j$
return p { p est la valeur de ab }

L'exemple 10 illustre l'utilisation de cet algorithme.

EXEMPLE 10 Trouver le produit de $a = (110)_2$ et $b = (101)_2$.

Solution: notez d'abord que

$$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2,$$

$$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2,$$

et

$$ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2.$$

Pour trouver le produit, ajoutez $(110)_2$, $(0000)_2$ et $(11000)_2$. Effectuer ces ajouts (us- L'algorithme 2, y compris les bits de zéro initiaux si nécessaire) montre que $ab = (1\,1110)_2$. Cette la multiplication est affichée dans la figure 2. ▲

$$\begin{array}{r} 110 \\ \times\ 101 \\ \hline 110 \\ 000 \\ 110 \\ \hline 11110 \end{array}$$

FIGURE 2 **Multiplier $(110)_2$ et $(101)_2$.**

Ensuite, nous déterminons le nombre d'additions de bits et de décalages de bits utilisés par l'algorithme 3 pour multiplier deux entiers.

EXEMPLE 11 Combien d'ajouts de bits et de décalages de bits sont utilisés pour multiplier a et b en utilisant l'algorithme 3?

Solution: l' algorithme 3 calcule les produits de a et b en ajoutant les produits partiels $c_0, c_1, c_2, \ldots$ et c_{n-1}. Lorsque $b_j = 1$, on calcule le produit partiel c_j en décalant le binaire expansion de a par j bits. Lorsque $b_j = 0$, aucun décalage n'est nécessaire car $c_j = 0$. Par conséquent, pour trouver tous les n entiers $ab_j 2^j$, $j = 0, 1, ..., n - 1$, nécessite au plus

$$0 + 1 + 2 + \cdots + n - 1$$

changements. Par conséquent, dans l'exemple 5 de la section 3.2, le nombre de décalages requis est $O(n^2)$.

Pour ajouter les entiers ab_j de $j = 0$ à $j = n - 1$ nécessite l'ajout d'un entier à n bits, un entier $(n + 1)$ bits, ..., et un entier $(2n)$ bits. Nous savons par l'exemple 9 que chacun de ces les additions nécessitent $O(n)$ additions de bits. Par conséquent, un total de $O(n^2)$ additions de bits sont requis pour tous les n ajouts. ▲

Étonnamment, il existe des algorithmes plus efficaces que l'algorithme conventionnel pour les tiplier des entiers. Un tel algorithme, qui utilise $O(n^{1.585})$ bit pour des opérations de multiplication n bits seront décrits à la section 8.3.

ALGORITHME POUR div ET mod Étant donné les entiers a et d, $d > 0$, nous pouvons trouver $q = a$ **div** d et $r = a$ **mod** d en utilisant l'algorithme 4. Dans cet algorithme de force brute, quand a est positive nous soustrayons d d' *un* autant de fois que nécessaire jusqu'à ce que ce qui reste est inférieure à d. le nombre de fois où nous effectuons cette soustraction est le quotient et ce qui reste après tous ces les soustractions sont le reste. L'algorithme 4 couvre également le cas où a est négatif. Cette algorithm trouve le quotient q et le reste r quand $|a|$ est divisé par d. Ensuite, quand $a < 0$ et $r > 0$, il les utilise pour trouver le quotient $-(q + 1)$ et le reste $d - r$ lorsque a est divisé par d.

Nous laissons au lecteur (Exercice 59) le soin de montrer que, en supposant que $a > d$, cet algorithme utilise Opérations sur les bits $O(q \log a)$.

ALGORITHME 4 Calcul div et mod.

algorithme de division de **procédure** (a : entier, d : entier positif)
$q := 0$
$r := |a|$
tandis que $r \geq d$
    $r := r - d$
    $q := q + 1$
si $a < 0$ et $r > 0$ **alors**
    $r := d - r$
    $q := -(q + 1)$
return (q, r) { $q = a$ **div** d est le quotient, $r = a$ **mod** d est le reste}

Il existe des algorithmes plus efficaces que l'algorithme 4 pour déterminer le quotient $q = a$ **div** d et le reste $r = a$ **mod** d lorsqu'un entier positif a est divisé par un positif entier d (voir [Kn98] pour plus de détails). Ces algorithmes nécessitent des opérations sur les bits $O(\log a \cdot \log d)$. Si les deux extensions binaires de a et d contiennent n bits ou moins, alors nous pouvons remplacer $\log a \cdot \log d$ par n^2. Cela signifie que nous avons besoin d'opérations sur $O(n^2)$ bits pour trouver le quotient et le reste lorsque a est divisé par d.

Exponentiation modulaire

En cryptographie, il est important de pouvoir trouver b^n **mod** m efficacement, où b, n et m sont grands entiers. Il est impossible de calculer d'abord b^n puis trouver son reste lorsqu'il est divisé par m parce que b^n sera un nombre énorme. Au lieu de cela, nous pouvons utiliser un algorithme qui utilise le expansion binaire de l'exposant n.

Avant de présenter cet algorithme, nous illustrons son idée de base. Nous expliquerons comment utiliser l'expansion binaire de n, disons $n = (a_{k-1} \dots a_1 a_0)_2$, pour calculer b^n. Tout d'abord, notez que

$$b^n = b^{a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \cdots b^{a_1 \cdot 2} \cdot b^{a_0}.$$

Cela montre que pour calculer b^n, il suffit de calculer les valeurs de b, b^2, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$, ..., b^{2^k}. Une fois que nous avons ces valeurs, nous multiplions les termes b^{2^j} dans cette liste, où $a_j = 1$. (Pour efficacité, après multiplication par chaque terme, on réduit le résultat modulo m.) Cela nous donne b^n. Pour Par exemple, pour calculer 3^{11}, nous notons d'abord que $11 = (1011)_2$, de sorte que $3^{11} = 3^8 3^2 3^1$. Par successivement au carré, nous constatons que $3^2 = 9$, $3^4 = 9^2 = 81$ et $3^8 = (81)^2 = 6561$. Par conséquent, $3^{11} = 3^8 3^2 3^1 = 6561 \cdot 9 \cdot 3 = 177, 147$.

L'algorithme trouve successivement b **mod** m , b^2 **mod** m , b^4 **mod** m, ..., $b^{2^{k-1}}$ **mod** m et multiplie ces termes b^{2^j} **mod** m où $a_j = 1$, trouver le reste du produit lorsqu'il est divisé par m après chaque multiplication. Pseudocode pour cet algorithme est montré dans l'algorithme 5. Notez que dans l'algorithme 5, nous pouvons utiliser l'algorithme le plus efficace disponible pour calculer les valeurs de la fonction **mod** , pas nécessairement l'algorithme 4.

Assurez-vous de réduire modulo *m* après chaque multiplication!

ALGORITHME 5 Exponentiation modulaire.

exponentiation modulaire de **procédure** (b : entier, $n = (a_{k-1} a_{k-2} \ldots a_1 a_0)_2$,
m : entiers positifs)
x : = 1
puissance : = b **mod** m
pour i : = 0 **à** k - 1
  si $a_i = 1$ **alors** x : = $(x \cdot$ *puissance*) **mod** m
  puissance : = (*puissance* · *puissance*) **mod** m
renvoie x { x est égal à b^n **mod** m }

Nous illustrons le fonctionnement de l'algorithme 5 dans l'exemple 12.

EXEMPLE 12 Utilisez l'algorithme 5 pour trouver 3^{644} **mod** 645.

Solution: l' algorithme 5 définit initialement $x = 1$ et la *puissance* = 3 **mod** 645 = 3. Dans le calcul de 3^{644} **mod** 645, cet algorithme détermine 3^{2^j} **mod** 645 pour $j = 1, 2, \ldots, 9$ par successivement quadrature et réduction du modulo 645. Si $a_j = 1$ (où a_j est le bit en j ème position dans le expansion binaire de 644, qui est $(1010000100)_2$), il multiplie la valeur actuelle de x par 3^{2^j} **mod** 645 et réduit le résultat modulo 645. Voici les étapes utilisées:

i = 0: Parce *que* $_0$ = 0, nous avons $x = 1$ et la *puissance* = 3^2 **mod** 645 = 9 **mod** 645 = 9;
i = 1: Parce *que* $_{1\ 1}$ = 0, nous avons $x = 1$ et la *puissance* = 9^2 **mod** 645 = 81 **mod** 645 = 81;
i = 2: Parce *que* $_2$ = 1, nous avons $x = 1 \cdot 81$ **mod** 645 = 81 et la *puissance* = 81^2 **mod** 645 = 6561 **mod** 645 = 111;
i = 3: Parce *que* $_3$ = 0, nous avons $x = 81$ et la *puissance* = 111^2 **mod** 645 = 12 , 321 **mod** 645 = 66;
i = 4: Parce *que* $_4$ = 0, nous avons $x = 81$ et la *puissance* = 66^2 **mod** 645 = 4356 **mod** 645 = 486;
i = 5: Parce *que* $_5$ = 0, nous avons $x = 81$ et la *puissance* = 486^2 **mod** 645 = 236 , 196 **mod** 645 = 126;
i = 6: Parce *que* $_6$ = 0, nous avons $x = 81$ et la *puissance* = 126^2 **mod** 645 = 15 , 876 **mod** 645 = 396;
i = 7: Parce *que* $_7$ = 1, nous trouvons que $x = (81 \cdot 396)$ **mod** 645 = 471 et *puissance* = 396^2 **mod** 645 = 156 , 816 **mod** 645 = 81;
i = 8: Parce *que* $_8$ = 0, nous avons $x = 471$ et *puissance* = 81^2 **mod** 645 = 6561 **mod** 645 = 111;
i = 9: Parce *que* $_9$ = 1, nous trouvons que $x = (471 \cdot 111)$ **mod** 645 = 36.

Cela montre que suivre les étapes de l'algorithme 5 produit le résultat 3^{644} **mod** 645 = 36. ▲

L'algorithme 5 est assez efficace; il utilise $O((\log m)^2 \log n)$ opérations binaires pour trouver b^n **mod** m (voir Exercice 58).

Des exercices

1. Convertissez l'expansion décimale de chacun de ces entiers à une expansion binaire.

a) 231 **b)** 4532 **c)** 97644

2. Convertissez l'expansion décimale de chacun de ces entiers à une expansion binaire.

a) 321 **b)** 1023 **c)** 100632

3. Convertissez l'expansion binaire de chacun de ces entiers en une expansion décimale.

a) $(1\ 1111)_2$ **b)** $(10\ 0000\ 0001)_2$
c) $(1\ 0101\ 0101)_2$ **d)** $(110\ 1001\ 0001\ 0000)_2$

4. Convertissez l'expansion binaire de chacun de ces entiers en une expansion décimale.

a) $(1\ 1011)_2$ **b)** $(10\ 1011\ 0101)_2$
c) $(11\ 1011\ 1110)_2$ **d)** $(111\ 1100\ 0001\ 1111)_2$

5. Convertissez l'expansion octale de chacun de ces entiers en un expansion binaire.

a) $(572)_8$ **b)** $(1604)_8$
c) $(423)_8$ **d)** $(2417)_8$

6. Convertissez l'expansion binaire de chacun de ces entiers en une expansion octale.

a) $(1111\ 0111)_2$
b) $(1010\ 1010\ 1010)_2$
c) $(111\ 0111\ 0111\ 0111)_2$
d) $(101\ 0101\ 0101\ 0101)_2$

7. Convertissez l'expansion hexadécimale de chacun de ces tegers à une expansion binaire.

a) $(80E)_{16}$ **b)** $(135AB)_{16}$
c) $(ABBA)_{16}$ **d)** (EFFACÉ)$_{16}$

8. Convertir $(BADFACED)_{16}$ à partir de son expansion hexadécimale à son expansion binaire.

9. Convertissez $(ABCDEF)_{16}$ de son expansion hexadécimale en son expansion binaire.

10. Convertissez chacun des entiers de l'exercice 6 à partir d'un binaire expansion à une expansion hexadécimale.

11. Convertissez $(1011\ 0111\ 1011)_2$ de son expansion binaire en son expansion hexadécimale.

12. Convertir $(1\ 1000\ 0110\ 0011)_2$ de son expansion binaire à son expansion hexadécimale.

13. Montrer que l'expansion hexadécimale d'un entier positif peut être obtenu à partir de son expansion binaire en regroupant des blocs gether de quatre chiffres binaires, ajoutant des zéros initiaux si nécessaire, et traduire chaque bloc de quatre chiffres binaires en un seul chiffre hexadécimal.

14. Montrer que l'expansion binaire d'un entier positif peut obtenu à partir de son expansion hexadécimale par traduction ing chaque chiffre hexadécimal dans un bloc de quatre binaires chiffres.

15. Montrer que l'expansion octale d'un entier positif peut être obtenu de son expansion binaire en regroupant blocs de trois chiffres binaires, en ajoutant des zéros initiaux si nécessaire essentiel, et traduire chaque bloc de trois chiffres binaires en un seul chiffre octal.

16. Montrer que l'expansion binaire d'un entier positif peut être obtenu à partir de son expansion octale en traduisant chaque chiffre octal en un bloc de trois chiffres binaires.

17. Convertir $(7345321)_8$ à son expansion binaire et $(10\ 1011\ 1011)_2$ à son expansion octale.

18. Donnez une procédure de conversion à partir de l'ex- expansion d'un entier à son expansion octale en utilisant binaire notation comme étape intermédiaire.

19. Donnez une procédure de conversion à partir de l'expansion octale d'un entier à son expansion hexadécimale en utilisant binaire notation comme étape intermédiaire.

20. Expliquez comment convertir une extension binaire en base 64 et des extensions de base 64 aux extensions binaires et des extensions octales à la base 64 et de la base 64 des extensions aux extensions octales.

21. Trouvez la somme et le produit de chacune de ces paires de Nombres. Exprimez vos réponses sous la forme d'une extension binaire.

a) $(100\ 0111)_2$, $(111\ 0111)_2$
b) $(1110\ 1111)_2$, $(1011\ 1101)_2$
c) $(10\ 1010\ 1010)_2$, $(1\ 1111\ 0000)_2$
d) $(10\ 0000\ 0001)_2$, $(11\ 1111\ 1111)_2$

22. Trouvez la somme et le produit de chacune de ces paires de nombres bers. Exprimez vos réponses sous la forme d'une extension de base 3.

a) $(112)_3$, $(210)_3$
b) $(2112)_3$, $(12021)_3$
c) $(20001)_3$, $(1111)_3$
d) $(120021)_3$, $(2002)_3$

23. Trouvez la somme et le produit de chacune de ces paires de nombres bers. Exprimez vos réponses sous la forme d'une extension octale.

a) $(763)_8$, $(147)_8$
b) $(6001)_8$, $(272)_8$
c) $(1111)_8$, $(777)_8$
d) $(54321)_8$, $(3456)_8$

24. Trouvez la somme et le produit de chacune de ces paires de nombres bers. Exprimez vos réponses sous la forme d'une extension hexadécimale sion.

a) $(1AE)_{16}$, $(BBC)_{16}$
b) $(20CBA)_{16}$, $(A01)_{16}$
c) $(ABCDE)_{16}$, $(1111)_{16}$
d) $(E0000E)_{16}$, $(BAAA)_{16}$

25. Utilisez l'algorithme 5 pour trouver 7^{644} **mod** 645.

26. Utilisez l'algorithme 5 pour trouver 11^{644} **mod** 645.

27. Utilisez l'algorithme 5 pour trouver 3^{2003} **mod** 99.

28. Utilisez l'algorithme 5 pour trouver 123^{1001} **mod** 101.

29. Montrer que chaque entier positif peut être représenté unique comme la somme des pouvoirs distincts de 2. [*Astuce:* Con- expansions binaires sider d'entiers.]

30. On peut montrer que chaque entier peut être représenté de façon unique envoyé dans le formulaire

$$e_k 3^k + e_{k-1} 3^{k-1} + \cdots + e_1 3 + e_0,$$

où $e_j = -1$, 0 ou 1 pour $j = 0 , 1 , 2 , ..., k$. Expan- de ce type sont appelées **expansions ternaires sions** . Trouvez les extensions ternaires équilibrées de

a) 5. **b)** 13. **c)** 37. **d)** 79.

31. Montrer qu'un entier positif est divisible par 3 si et seulement si la somme de ses chiffres décimaux est divisible par 3.

32. Montrer qu'un entier positif est divisible par 11 si et seulement si la différence de la somme de ses chiffres décimaux en positions numérotées et la somme de ses chiffres décimaux les positions impaires sont divisibles par 11.

33. Montrer qu'un entier positif est divisible par 3 si et seulement si la différence de la somme de ses chiffres binaires en positions numérotées et la somme de ses chiffres binaires les positions impaires sont divisibles par 3.

Les représentations **complémentaires** d'un entier sont utilisées pour simplifier l'arithmétique informatique. Représenter positif et négatif nombres entiers positifs dont la valeur absolue est inférieure à 2^{n-1}, un total de n bits est utilisé. Le bit le plus à gauche est utilisé pour représenter le signe. Un bit 0 dans cette position est utilisé pour les entiers positifs, et un bit dans ce position est utilisée pour les entiers négatifs. Pour les entiers positifs, les bits restants sont identiques à l'expansion binaire du entier. Pour les entiers négatifs, les bits restants sont obtenus en trouvant d'abord l'expansion binaire de la valeur absolue de l'entier, puis en prenant le complément de chacun de ces bits, où le complément d'un 1 est un 0 et le complément d'un 0 est un 1.

34. Trouver les représentations du complément à un, en utilisant bit chaînes de longueur six, des entiers suivants.

a) 22 **b)** 31 **c)** −7 **d)** −19

35. Quel entier chacun des éléments suivants complète-t-il que représentent les représentations de longueur cinq?

a) 11001 **b)** 01101

c) 10001 **d)** 11111

36. Si m est un entier positif inférieur à 2^{n-1}, comment est la sa représentation du complément de $-m$ obtenue à partir de le complément à un de m , lorsque les chaînes de bits de longueur n sont utilisés?

37. Comment est la représentation du complément à un de la somme de deux nombres entiers obtenus à partir du complément à un ressentiments de ces nombres entiers?

38. Comment est la représentation complémentaire des différences de deux entiers obtenus à partir du complément à un représentations de ces nombres entiers?

39. Montrer que l'entier m avec son complément représentation $(a_{n-1} a_{n-2} \ldots a_1 a_0)$ peut être trouvée dans l'équation $m = -a_{n-1}(2^{n-1} - 1) + a_{n-2} 2^{n-2} + \cdots + a_1 \cdot 2 + a_0$.

Les représentations du **complément à deux** d'entiers sont également utilisées pour simplifier l'arithmétique informatique et sont plus couramment utilisés que ses représentations complémentaires. Pour représenter un ger x avec $-2^{n-1} \leq x \leq 2^{n-1} - 1$ pour un positif spécifié entier n , un total de n bits est utilisé. Le bit le plus à gauche est utilisé pour représenter le signe. Un bit 0 dans cette position est utilisé pour le positif entiers, et un bit de 1 dans cette position est utilisé pour les entiers négatifs comme dans les extensions de son complément. Pour un positif entier, les bits restants sont identiques à l'expansion binaire sion de l'entier. Pour un entier négatif, les bits restants sont les bits de l'expansion binaire de $2^{n-1} - |x|$. Deux com- les extensions complètes d'entiers sont souvent utilisées par les ordinateurs parce que l'addition et la soustraction d'entiers peuvent être effectuées en utilisant facilement ces extensions, où ces entiers peuvent être ei- il est positif ou négatif.

40. Répondez à l'exercice 34, mais cette fois, trouvez les deux l'expansion de ment à l'aide de chaînes de bits de longueur six.

41. Répondez à l'exercice 35 si chaque extension est un complément à deux élargissement de la longueur cinq.

42. Répondez à l'exercice 36 pour les extensions de complément à deux.

43. Répondez à l'exercice 37 pour les extensions de complément à deux.

44. Répondez à l'exercice 38 pour les extensions du complément à deux.

45. Montrer que l'entier m avec complément à deux représentation $(a_{n-1} a_{n-2} \ldots a_1 a_0)$ peut être trouvée dans l'équation $m = -a_{n-1} \cdot 2^{n-1} + a_{n-2} 2^{n-2} + \cdots + a_1 \cdot 2 + a_0$.

46. Donnez un algorithme simple pour former les deux compléments. représentation d'un entier à partir de son ensemble représentation du gouvernement.

47. Parfois, les nombres entiers sont codés en utilisant des extensions nécessaires pour représenter chaque chiffre décimal. Ce pro- réduit la **forme décimale codée binaire** de l'entier. Pour par exemple, 791 est codé de cette manière par 011110010001. Combien de bits sont nécessaires pour représenter un nombre avec n chiffres décimaux utilisant ce type de codage?

Une **extension Cantor** est une somme de la forme

$$a_n n! + a_{n-1}(n-1)! + \cdots + a_2 2! + un_1 1!,$$

où a_i est un entier avec $0 \leq a_i \leq i$ pour $i = 1 , 2 , ..., n$.

48. Trouvez les extensions Cantor de

a) 2. **b)** 7.

c) 19. **d)** 87.

e) 1000. **f)** 1 000 000.

∗ **49.** Décrire un algorithme qui trouve l'extension Cantor de un nombre entier.

∗ **50.** Décrire un algorithme pour ajouter deux entiers à partir de leur expansions.

51. Ajoutez $(10111)_2$ et $(11010)_2$ en parcourant chacun étape de l'algorithme d'addition donnée dans le texte.

52. Multipliez $(1110)_2$ et $(1010)_2$ en passant par chacun étape de l'algorithme de multiplication donnée dans le texte.

53. Décrire un algorithme pour trouver la différence de deux expansions binaires.

54. Estimer le nombre d'opérations binaires utilisées pour soustraire deux extensions binaires.

55. Concevoir un algorithme qui, compte tenu des extensions binaires de les entiers a et b , détermine si $a > b$, $a = b$, ou $a < b$.

56. Combien d'opérations sur bits la comparaison algorithme de l'exercice 55 à utiliser lorsque le plus grand de a et b a n bits dans son expansion binaire?

57. Estimer la complexité de l'algorithme 1 pour trouver le base b expansion d'un entier n en termes de nombre des divisions utilisées.

∗ **58.** Montrer que l'algorithme 5 utilise l' opération de bit $O((\log m)^2 \log n)$ pour trouver b^n **mod** m .

59. Montrer que l'algorithme 4 utilise des opérations sur les bits $O(q \log a)$, en supposant que $a > d$.

Les nombres premiers et les plus grands diviseurs communs

introduction

Dans la section 4.1, nous avons étudié le concept de divisibilité des nombres entiers.Un concept important basé la divisibilité est celle d'un nombre premier. Un nombre premier est un entier supérieur à 1 qui est divisible par pas d'entiers positifs autres que 1 et lui-même.L'étude des nombres premiers remonte à l'ancien fois. Il y a des milliers d'années, on savait qu'il existe une infinité de nombres premiers;la preuve de ce fait, trouvé dans les œuvres d'Euclide, est célèbre pour son élégance et sa beauté.

Nous discuterons de la distribution des nombres premiers parmi les entiers.Nous décrirons certains des résultats sur les nombres premiers trouvés par les mathématiciens au cours des 400 dernières années.En particulier, nous introduira un théorème important, le théorème fondamental de l'arithmétique.Ce théorème, qui affirme que chaque entier positif peut être écrit uniquement comme le produit de nombres premiers dans ordre non décroissant, a de nombreuses conséquences intéressantes. Nous discuterons également de quelques-uns des nombreux vieilles conjectures sur les nombres premiers qui ne sont toujours pas réglées aujourd'hui.

Les amorces sont devenues essentielles dans les systèmes cryptographiques modernes, et nous développerons de leurs propriétés importantes en cryptographie.Par exemple, trouver de grands nombres premiers est essentiel dans cryptographie moderne. La durée nécessaire pour factoriser de grands nombres entiers dans leurs facteurs premiers est la base de la force de certains systèmes cryptographiques modernes importants.

Dans cette section, nous étudierons également le plus grand diviseur commun de deux nombres entiers, ainsi que le le plus petit commun multiple de deux entiers.Nous développerons un algorithme important pour le calcul les plus grands diviseurs communs, appelés algorithme euclidien.

Primes

Chaque entier supérieur à 1 est divisible par au moins deux entiers, car un entier positif est divisible par 1 et par lui-même. Entiers positifs qui ont exactement deux entiers positifs différents les facteurs sont appelés **nombres premiers** .

DÉFINITION 1 Un entier p supérieur à 1 est appelé *premier* si les seuls facteurs positifs de p sont 1 et p . Un entier positif supérieur à 1 et non premier est appelé *composite* .

Remarque: l'entier n est composite si et seulement s'il existe un entier a tel que $a \mid n$ et $1 < a < n$.

EXEMPLE 1 L'entier 7 est premier car ses seuls facteurs positifs sont 1 et 7, tandis que l'entier 9 est composite car il est divisible par 3. ▲

Les nombres premiers sont les éléments constitutifs d'entiers positifs, comme le théorème fondamental de spectacles arithmétiques. La preuve sera donnée dans la section 5.2.

THÉORÈME 1 **LE THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE** Chaque entier supérieur à 1 peut être écrit uniquement comme un nombre premier ou comme le produit de deux nombres premiers ou plus où le nombre premier les facteurs sont écrits par ordre de taille non décroissante.

L'exemple 2 donne quelques factorisations premières d'entiers.

EXEMPLE 2 Les facteurs premiers de 100, 641, 999 et 1024 sont donnés par

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,

$641 = 641$,

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$,

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$. ▲

Division de première instance

Il est souvent important de montrer qu'un entier donné est premier. Par exemple, en cryptologie, les grands les nombres premiers sont utilisés dans certaines méthodes pour rendre les messages secrets. Une procédure pour montrer que un entier est premier est basé sur l'observation suivante.

THÉORÈME 2 Si n est un entier composite, alors n a un diviseur premier inférieur ou égal à $\sqrt{n}$.

Preuve: si n est composite, par la définition d'un entier composite, on sait qu'il a un facteur a avec $1 < a < n$. Par conséquent, par la définition d'un facteur d'un entier positif, nous avons $n = ab$, où b est un entier positif supérieur à 1. Nous montrerons que $a \le \sqrt{n}$ ou $b \le \sqrt{n}$. Si $a > \sqrt{n}$ et $b > \sqrt{n}$, puis $ab > \sqrt{n} \cdot \sqrt{n} = n$, ce qui est une contradiction. Par conséquent, $a \le \sqrt{n}$ ou $b \le \sqrt{n}$. Parce que a et b sont tous les deux des diviseurs de n, nous voyons que n a un diviseur positif ne dépassant pas $\sqrt{n}$. Ce diviseur est premier ou, selon le théorème fondamental de l'arithmétique, a un diviseur premier moins que lui-même. Dans les deux cas, n a un diviseur premier inférieur ou égal à $\sqrt{n}$.

Du théorème 2, il s'ensuit qu'un entier est premier s'il n'est pas divisible par un nombre premier moins supérieur ou égal à sa racine carrée. Cela conduit à l'algorithme de force brute connu sous le nom de **division d'essai**. Pour utiliser la division d'essai, nous divisons n par tous les nombres premiers ne dépassant pas $\sqrt{n}$ et conclure que n est premier s'il n'est divisible par aucun de ces nombres premiers. Dans l'exemple 3, nous utilisons la division d'essai pour montrer que 101 est premier.

EXEMPLE 3 Montrez que 101 est premier.

Solution: les seuls nombres premiers ne dépassant pas $\sqrt{101}$ sont 2, 3, 5 et 7. Parce que 101 n'est pas divisible par 2, 3, 5 ou 7 (le quotient de 101 et chacun de ces entiers n'est pas un entier), il s'ensuit que 101 est premier. ▲

Parce que chaque entier a une factorisation première, il serait utile d'avoir une procédure pour trouver cette factorisation première. Considérons le problème de la recherche de la factorisation en nombres premiers de n. Commencez par diviser n par des nombres premiers successifs, en commençant par le plus petit nombre premier, 2. Si n a un nombre premier facteur, puis par le théorème 3 un facteur premier p ne dépassant pas $\sqrt{n}$ sera trouvé. Donc, si pas de prime

facteur ne dépassant pas $\sqrt{n}$ est trouvé, alors n est premier. Sinon, si un facteur premier p est trouvé, continuer en factorisant n / p. Notez que n / p n'a pas de facteurs premiers inférieurs à p. Encore une fois, si n / p a pas de facteur premier supérieur ou égal à p et ne dépassant pas sa racine carrée, alors il est premier. Sinon, s'il a un facteur premier q, continuez en factorisant $n / (pq)$. Cette procédure se poursuit jusqu'à ce que la factorisation soit réduite à un nombre premier. Cette procédure est illustrée dans l'exemple 4.

EXEMPLE 4 Trouver la factorisation en nombres premiers de 7007.

Solution: pour trouver la factorisation de 7007, effectuez d'abord des divisions de 7007 par nombres premiers, commençant par 2. Aucun des nombres premiers 2, 3 et 5 ne divise 7007. Cependant, 7 VIDES 7007, avec $7\,007 / 7 = 1001$. Ensuite, divisez 1001 par des nombres premiers successifs, en commençant par 7. On voit immédiatement que 7 divise également 1001, parce que $1001/ 7 = 143$. Continuez en divisant 143 par nombres premiers successifs, en commençant par 7. Bien que 7 ne divise pas 143, 11 ne diviser 143 et $143 / 11 = 13$. Parce que 13 est premier, la procédure est terminée. Il s'ensuit que $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Par conséquent, la décomposition en facteurs premiers de 7007 est $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ▲

Les nombres premiers ont été étudiés dans les temps anciens pour des raisons philosophiques. Aujourd'hui, il y a raisons très pratiques de leur étude. En particulier, les grands nombres premiers jouent un rôle crucial dans la cryptographie. tography, comme nous le verrons dans la section 4.6.

Le tamis d'Ératosthène

Notez que les entiers composites ne dépassant pas 100 doivent avoir un facteur premier ne dépassant pas 10.

Parce que les seuls nombres premiers inférieurs à 10 sont 2, 3, 5 et 7, les nombres premiers ne dépassant pas 100 sont ceux-ci quatre nombres premiers et les entiers positifs supérieurs à 1 et n'excédant pas 100 divisibles par aucun de 2, 3, 5 ou 7.

Le **tamis d'Eratosthène** est utilisé pour trouver tous les nombres premiers ne dépassant pas un positif spécifié entier. Par exemple, la procédure suivante est utilisée pour trouver les nombres premiers ne dépassant pas 100. Nous commencer par la liste de tous les entiers compris entre 1 et 100. Pour commencer le processus de tamisage, les entiers qui sont divisibles par 2, autres que 2, sont supprimés. Parce que 3 est le premier entier supérieur à 2 qui est laissé, tous ces entiers divisibles par 3, autres que 3, sont supprimés. Parce que 5 est le prochain entier à gauche après 3, ces entiers divisibles par 5, autres que 5, sont supprimés. Le prochain entier à gauche est 7, donc ces entiers divisibles par 7, autres que 7, sont supprimés. Parce que tous les entiers composites ne sont pas supérieur à 100 sont divisibles par 2, 3, 5 ou 7, tous les entiers restants sauf 1 sont premiers. Dans le tableau 1, les panneaux affichent les entiers supprimés à chaque étape, où chaque entier divisible par 2, autre supérieur à 2, est souligné dans le premier panneau, chaque entier divisible par 3, autre que 3, est souligné dans le deuxième panneau, chaque entier divisible par 5, autre que 5, est souligné dans le troisième panneau, et chaque entier divisible par 7, autre que 7, est souligné dans le quatrième panneau. Les entiers non les nombres premiers ne dépassant pas 100 sont soulignés. Nous concluons que les nombres premiers inférieurs à 100 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.

L'INFINITUDE DES PRIMES On sait depuis longtemps qu'il existe une infinité de nombres premiers. Cela signifie que chaque fois que $p_1, p_2, \ldots, p_n$ sont les n plus petits nombres premiers, nous savons qu'il y a un plus grand

ÉRATOSTHÈNE (276 AEC – 194 AEC) On sait qu'Ératosthène est né à Cyrène, une colonie grecque à l'ouest de l'Égypte, et a passé du temps à étudier à l'Académie Platon à Athènes. Nous savons également que le roi Ptolémée II invité Eratosthène à Alexandrie pour donner des cours particuliers à son fils et que plus tard Eratosthène est devenu bibliothécaire célèbre bibliothèque d'Alexandrie, un dépôt central de la sagesse ancienne. Eratosthenes était extrêmement polyvalent érudit, écrit sur les mathématiques, la géographie, l'astronomie, l'histoire, la philosophie et la critique littéraire. Outre son travail en mathématiques, il est surtout connu pour sa chronologie de l'histoire ancienne et pour sa célèbre mesure de la taille de la terre.

TABLEAU 1 Le tamis d'Ératosthène.

Entiers divisibles par 2 autres que 2 recevoir un soulignement.

1	2	3	4	5	6	sept	8	9	dix
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Entiers divisibles par 3 autres que 3 recevoir un soulignement.

1	2	3	4	5	6	sept	8	9	dix
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Entiers divisibles par 5 autres que 5 recevoir un soulignement.

1	2	3	4	5	6	sept	8	9	dix
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Entiers divisibles par 7 autres que 7 reçoivent un soulignement; les entiers en couleur sont premiers.

1	2	3	4	5	6	sept	8	9	dix
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

premier non répertorié. Nous prouverons ce fait en utilisant une preuve donnée par Euclide dans ses célèbres mathématiques texte, *Les éléments* . Cette preuve simple mais élégante est considérée par de nombreux mathématiciens comme parmi les plus belles preuves en mathématiques. Il s'agit de la première preuve présentée dans le livre *Preuves de THE BOOK* [AiZi10], où THE BOOK fait référence à la collection imaginée de preuves parfaites que le célèbre mathématicien Paul Erd˝os a affirmé est maintenu par Dieu. Au fait, il y a sont un grand nombre de preuves différentes qu'il y a une infinité de nombres premiers, et de nouvelles sont publié étonnamment fréquemment.

THÉORÈME 3 Il existe une infinité de nombres premiers.

Preuve: Nous allons prouver ce théorème en utilisant une preuve par contradiction. Nous supposons qu'il n'y a que nombre fini de nombres premiers, $p_1, p_2, \ldots, p_n$. Laisser

$$Q = p_1 p_2 \cdots p_n + 1.$$

Par le théorème fondamental de l'arithmétique, Q est premier ou bien il peut être écrit comme le produit de deux nombres premiers ou plus. Cependant, aucun des nombres premiers p_j ne divise Q, car si $p_j \mid Q$, alors p_j divise

$Q - p_1 p_2 \cdots p_n = 1$. Il n'y a donc pas de nombre premier dans la liste $p_1, p_2, \ldots, p_n$. Ce premier est soit Q, si elle est premier, ou un facteur premier de Q. Ceci est une contradiction parce que nous avons supposé que nous avons répertorié tous les nombres premiers. Par conséquent, il existe une infinité de nombres premiers.

Remarque: Notez que dans cette preuve nous n'affirmons *pas* que Q est premier! De plus, dans cette preuve, nous ont donné une preuve d'existence non constructive que, étant donné tout n nombre premier, il n'y a pas de nombre premier dans cette liste. Pour que cette preuve soit constructive, il aurait fallu donner explicitement un nombre premier non notre liste originale de n nombres premiers.

Parce qu'il y a une infinité de nombres premiers, étant donné tout entier positif, il y a des nombres premiers supérieurs que cet entier. Il y a une quête continue pour découvrir des nombres premiers de plus en plus grands; pour presque tous les 300 dernières années, le plus grand nombre premier connu a été un entier de la forme spéciale $2^p - 1$, où p est également premier. (Notez que $2^n - 1$ ne peut pas être premier lorsque n n'est pas premier; voir Exercice 9.) Ces nombres premiers sont appelés **nombres premiers de Mersenne**, d'après le moine français Marin Mersenne, qui les a étudiés au XVIIe siècle. La raison pour laquelle le plus grand nombre premier connu a généralement été un premier Mersenne est qu'il existe un test extrêmement efficace, connu sous le nom de Lucas – Lehmer test, pour déterminer si $2^p - 1$ est premier. De plus, il n'est actuellement pas possible de tester les numéros qui ne sont pas de cette forme ou de certaines autres formes spéciales n'importe où près aussi rapidement pour déterminer si ils sont premiers.

EXEMPLE 5 Les nombres $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ et $2^7 - 1 = 127$ sont des nombres premiers de Mersenne, tandis que $2^{11} - 1 = 2047$ n'est pas un nombre premier de Mersenne car $2047 = 23 \cdot 89$. ▲

Les progrès dans la recherche de nombres premiers de Mersenne sont stables depuis l'invention des ordinateurs. Au début 2011, 47 nombres premiers de Mersenne étaient connus, dont 16 trouvés depuis 1990. Le plus grand Mersenne le nombre premier connu (à nouveau au début de 2011) est de $2^{43,112,609} - 1$, un nombre avec près de 13 millions de décimales chiffres, qui s'est avéré être premier en 2008. Un effort commun, le Grand Internet Mersenne Prime Search (GIMPS), est consacré à la recherche de nouveaux nombres premiers de Mersenne. Vous pouvez rejoindre ce recherchez, et si vous avez de la chance, trouvez un nouveau Mersenne prime et peut-être même gagnez un prix en argent. Par en fait, même la recherche de nombres premiers de Mersenne a des implications pratiques. Un test de contrôle qualité pour les superordinateurs a consisté à reproduire le test de Lucas – Lehmer qui établit la primauté de un grand Mersenne prime. (Voir [Ro10] pour plus d'informations sur la quête de la découverte de Mersenne nombres premiers.)

LA DISTRIBUTION DES PRIMES Le théorème 3 nous dit qu'il existe une infinité de nombres premiers. Cependant, combien de nombres premiers sont inférieurs à un nombre positif x ? Cette question intéressait maticiens depuis de nombreuses années; à la fin du XVIIIe siècle, les mathématiciens ont produit de grandes tables

MARIN MERSENNE (1588-1648) Mersenne est né dans le Maine, en France, dans une famille d'ouvriers et a fréquenté le Collège du Mans et le Collège des Jésuites de La Flèche. Il a poursuivi ses études au Sorbonne, étudie la théologie de 1609 à 1611. Il rejoint l'ordre religieux des Minimes en 1611, un groupe dont le nom vient du mot *minimi* (les membres de ce groupe étaient extrêmement humbles; ils considéraient se sont érigés le moins de tous les ordres religieux). Outre la prière, les membres de ce groupe ont consacré leur énergie à l'érudition et à l'étude. En 1612, il devient prêtre place Royale à Paris; entre 1614 et En 1618, il enseigne la philosophie au couvent Minim de Nevers. Il revient à Paris en 1619, où sa cellule dans les Minims de l'Annociade est devenu un lieu de rencontres de scientifiques, philosophes et mathématiciens français maticiens, dont Fermat et Pascal. Mersenne a beaucoup correspondu avec des universitaires de toute l'Europe, servir de centre d'échange pour les connaissances mathématiques et scientifiques, une fonction remplie plus tard par des revues mathématiques (et aujourd'hui également par Internet). Mersenne a écrit des livres couvrant la mécanique, la physique mathématique, les mathématiques, la musique et l'acoustique. Il étudié les nombres premiers et essayé en vain de construire une formule représentant tous les nombres premiers. En 1644, Mersenne a affirmé que $2^p - 1$ est premier pour $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ mais est composite pour tous les autres nombres premiers inférieurs à 257. Il a pris plus de 300 ans pour déterminer que la demande de Mersenne était erronée cinq fois. Plus précisément, $2^p - 1$ n'est pas premier pour $p = 67$ et $p = 257$ mais est premier pour $p = 61$, $p = 87$ et $p = 107$. Il convient également de noter que Mersenne a défendu deux des hommes les plus célèbres de son temps, Descartes et Galileo, de critiques religieux. Il a également contribué à dénoncer les alchimistes et les astrologues comme des fraudes.

des nombres premiers pour recueillir des preuves concernant la distribution des nombres premiers. En utilisant ces preuves, les grands mathématiciens de l'époque, dont Gauss et Legendre, ont conjecturé, mais n'ont pas prouver, Théorème 4.

THÉORÈME 4 **LE THÉORÈME DU NOMBRE PRIME** Le rapport du nombre de nombres premiers ne dépassant pas x et $x / \ln x$ approchent 1 lorsque x croît sans limite. (Ici $\ln x$ est le logarithme naturel de x .)

Le théorème des nombres premiers a été prouvé pour la première fois en 1896 par le mathématicien français Jacques Hadamard et le mathématicien belge Charles-Jean-Gustave-Nicholas de la Vallée-Poussin en utilisant la théorie des variables complexes. Bien que les preuves n'utilisant pas de variables complexes aient été trouvé, toutes les preuves connues du théorème des nombres premiers sont assez compliquées.

Nous pouvons utiliser le théorème des nombres premiers pour estimer les chances qu'un nombre choisi au hasard est premier. Le théorème des nombres premiers nous dit que le nombre de nombres premiers ne dépassant pas x peut être approximée par $x / \ln x$. Par conséquent, les chances qu'un entier positif sélectionné au hasard moins que n est premier sont approximativement $(n / \ln n) / n = 1 / \ln n$. Parfois, nous devons trouver un premier avec un nombre particulier de chiffres. Nous aimerions une estimation du nombre d'entiers avec un nombre particulier de chiffres que nous devons sélectionner avant de rencontrer un nombre premier. Utiliser le premier théorème des nombres et calcul, on peut montrer que la probabilité qu'un entier n soit premier est également d'environ $1 / \ln n$. Par exemple, les probabilités qu'un entier proche de 10^{1000} soit premier sont environ $1 / \ln 10^{1000}$, soit environ 1 / 2300. (Bien sûr, en choisissant uniquement nous doublons nos chances de trouver un nombre premier.)

L'utilisation de la division d'essai avec le théorème 2 donne des procédures pour l'affacturage et pour le test de primalité. Cependant, ces procédures ne sont pas des algorithmes efficaces; beaucoup plus pratique et efficace des algorithmes pour ces tâches ont été développés. L'affacturage et les tests de primalité sont devenus important dans les applications de la théorie des nombres à la cryptographie. Cela a suscité un grand intérêt dans le développement d'algorithmes efficaces pour les deux tâches. Des procédures intelligentes ont été conçues 30 dernières années pour générer efficacement de grands nombres premiers. De plus, en 2002, un important la découverte a été faite par Manindra Agrawal, Neeraj Kayal et Nitin Saxena. Ils y ont montré est un algorithme à temps polynomial du nombre de bits dans l'expansion binaire d'un entier pour déterminer si un entier positif est premier. Les algorithmes basés sur leur travail utilisent $O((\log n)^6)$ opérations binaires pour déterminer si un entier positif n est premier.

Cependant, même si de nouvelles méthodes de factorisation puissantes ont été développées Dans le même laps de temps, la prise en compte de grands nombres reste extraordinairement plus longue que test de primalité. Aucun algorithme polynomial pour la factorisation d'entiers n'est connu. Cependant, le défi de l'affacturage en grand nombre intéresse de nombreuses personnes. Il y a un effort commun sur Internet pour factoriser les grands nombres, en particulier ceux de la forme spéciale $k^n \pm 1$, où k est un petit entier positif et n est un grand entier positif (ces nombres sont appelés *Cunningham chiffres*). À tout moment, il existe une liste des «dix personnes les plus recherchées» de ce type en attente de factorisation.

PRIMES ET PROGRESSIONS ARITHMÉTIQUES Chaque entier impair est dans l'un des deux progressions arithmétiques $4k + 1$ ou $4k + 3$, $k = 1, 2, \ldots$. Parce qu'on sait qu'il y a infiniment de nombreux nombres premiers, nous pouvons nous demander s'il existe une infinité de nombres premiers dans ces deux arithmétiques progressions. Les nombres premiers 5, 13, 17, 29, 37, 41, ... sont dans la progression arithmétique $4k + 1$; les nombres premiers 3, 7, 11, 19, 23, 31, 43, ... sont dans la progression arithmétique $4k + 3$. En regardant les preuves suggèrent qu'il peut y avoir une infinité de nombres premiers dans les deux progressions. Qu'en est-il de autres progressions arithmétiques $ak + b$, $k = 1, 2, \ldots$, où aucun entier supérieur à un ne divise à la fois *un* et b ? Contiennent-ils une infinité de nombres premiers? La réponse a été fournie par mathématicien G. Lejeune Dirichlet, qui a prouvé que chaque progression arithmétique contient infiniment de nombres premiers. Sa preuve, et toutes les preuves trouvées plus tard, sortent du cadre de ce livre.

Cependant, il est possible de prouver des cas particuliers du théorème de Dirichlet en utilisant les idées développées dans ce livre. Par exemple, les exercices 54 et 55 demandent des preuves qu'il existe une infinité de premiers dans les progressions arithmétiques $3k + 2$ et $4k + 3$, où k est un entier positif. (L'indice pour chacun de ces exercices fournit l'idée de base nécessaire à la preuve.)

Nous avons expliqué que chaque progression arithmétique $ak + b$, $k = 1, 2, \ldots$, où a et b n'ont pas de facteur commun supérieur à un, contient une infinité de nombres premiers. Mais y a-t-il longtemps progressions arithmétiques composées uniquement de nombres premiers? Par exemple, certaines explorations montrent que 5, 11, 17, 23, 29 est une progression arithmétique de cinq nombres premiers et 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 est une progression arithmétique de dix nombres premiers. Dans les années 1930, le célèbre le mathématicien Paul Erd˝os a supposé que pour chaque entier positif n supérieur à deux, il est une progression arithmétique de longueur n entièrement composée de nombres premiers. En 2006, Ben Green et Terence Tao a pu prouver cette conjecture. Leur preuve, considérée comme mathématique tour de force, est une preuve non constructive qui combine des idées puissantes de plusieurs avancées domaines des mathématiques.

Conjectures et problèmes ouverts sur les amorces

La théorie des nombres est considérée comme un sujet pour lequel il est facile de formuler des conjectures, dont certaines sont difficiles à prouver et d'autres qui sont restés des problèmes ouverts pendant de nombreuses années. Nous décrirons quelques conjectures dans la théorie des nombres et discuter de leur statut dans les exemples 6 à 9.

EXEMPLE 6 Il serait utile d'avoir une fonction $f(n)$ telle que $f(n)$ soit premier pour tous les entiers positifs n. Si nous avait une telle fonction, nous pouvions trouver de grands nombres premiers à utiliser dans la cryptographie et d'autres applications. À la recherche d'une telle fonction, nous pourrions vérifier différentes fonctions polynomiales, comme certains les mathématiciens l'ont fait il y a plusieurs centaines d'années. Après beaucoup de calculs, nous pouvons rencontrer le polynôme $f(n) = n^2 - n + 41$. Ce polynôme a la propriété intéressante que $f(n)$ est premier pour tous les entiers positifs n ne dépassant pas 40. [On a $f(1) = 41$, $f(2) = 43$, $f(3) = 47$, $f(4) = 53$, et ainsi de suite.] Cela peut nous conduire à la conjecture que $f(n)$ est premier pour tout positif entiers n. Pouvons-nous régler cette conjecture?

Solution: Sans surprise, cette conjecture s'avère fausse; nous n'avons pas à chercher loin pour trouver un entier positif n pour lequel $f(n)$ est composite, car $f(41) = 41^2 - 41 + 41 = 41^2$. Parce que $f(n) = n^2 - n + 41$ est premier pour tous les entiers positifs n avec $1 \leq n \leq 40$, nous pourrions

TERENCE TAO (NÉ EN 1975) Tao est né en Australie. Son père est pédiatre et sa mère a enseigné mathématiques dans une école secondaire de Hong Kong. Tao était un enfant prodige, s'enseignant l'arithmétique à l'âge de deux. À 10 ans, il est devenu le plus jeune candidat à l'Olympiade mathématique internationale (OMI); il a gagné une médaille d'or de l'OMI à 13 ans. Tao a obtenu son baccalauréat et sa maîtrise à 17 ans et a commencé ses études étudie à Princeton, recevant son doctorat. dans trois ans. En 1996, il est devenu membre du corps professoral de l'UCLA, où il continue de travailler.

Tao est extrêmement polyvalent; il aime travailler sur des problèmes dans divers domaines, y compris l'analyse harmonique sis, équations aux dérivées partielles, théorie des nombres et combinatoire. Vous pouvez suivre son travail en lisant son blog où il discute des progrès sur divers problèmes. Son résultat le plus célèbre est le théorème de Green-Tao, qui dit qu'il y a des progressions arithmétiques arbitrairement longues des nombres premiers. Tao a apporté une contribution importante aux applications des mathématiques, comme le développement d'une méthode de reconstruction d'images numériques en utilisant le moins d'informations possible. Tao a une réputation incroyable parmi les mathématiciens; il est devenu M. Fix-It pour les chercheurs en mathématiques. Le bien-connu le mathématicien Charles Fefferman, lui-même un enfant prodige, a déclaré que «si vous êtes coincé sur un problème, alors une solution consiste à intéresser Terence Tao. »En 2006, Tao a reçu la médaille Fields, le prix le plus prestigieux décerné aux mathématiciens de moins de 40 ans. a également reçu une bourse MacArthur en 2006, et en 2008, il a reçu le prix Allan T. Waterman, qui est venu avec un 500 000 $ en argent pour soutenir les travaux de recherche des scientifiques au début de leur carrière. Laura, la femme de Tao, est ingénieure au Jet Propulsion Laboratoire.

être tenté de trouver un polynôme différent avec la propriété que *f (n)* est premier pour *tout* positif entiers n . Cependant, il n'y a pas un tel polynôme. On peut montrer que pour chaque polynôme *f (n)* avec des coefficients entiers, il existe un entier positif y tel que *f (y)* est composite. (Voir Exercice 23 des exercices supplémentaires.) ▲

De nombreux problèmes célèbres concernant les nombres premiers attendent toujours une résolution finale par des gens intelligents. nous décrire quelques-uns des problèmes ouverts les plus accessibles et les mieux connus dans les exemples 7 à 9. La théorie des nombres est connue pour sa richesse de conjectures faciles à comprendre qui résistent à l'attaque de tous mais les techniques les plus sophistiquées, ou tout simplement résister à toutes les attaques. Nous présentons ces conjectures pour montrer que de nombreuses questions qui semblent relativement simples restent en suspens, même au XXI siècle.

EXEMPLE 7 **Conjecture de Goldbach** En 1742, Christian Goldbach, dans une lettre à Leonhard Euler, conjecturé que chaque entier impair n , $n > 5$, est la somme de trois nombres premiers. Euler a répondu que cette conjecture est équivalente à la conjecture que chaque entier pair n , $n > 2$, est la somme de deux nombres premiers (voir Exercice 21 des exercices supplémentaires). La conjecture que tout entier pair n , $n > 2$, est la somme de deux nombres premiers est maintenant appelée **conjecture de Goldbach** . Nous pouvons vérifier cette conjecture pour petits nombres pairs. Par exemple, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$, etc. La conjecture de Goldbach a été vérifiée par des calculs manuels pour des nombres lions avant l'avènement des ordinateurs. Avec les ordinateurs, il peut être vérifié Nombres. À la mi-2011, la conjecture a été vérifiée pour tous les entiers pairs positifs jusqu'à $1 . 6 \cdot 10^{18}$.

Bien qu'aucune preuve de la conjecture de Goldbach n'ait été trouvée, la plupart des mathématiciens pensent c'est vrai. Plusieurs théorèmes ont été prouvés, en utilisant des méthodes compliquées de nombre analytique théorie bien au-delà de la portée de ce livre, établissant des résultats plus faibles que la conjecture de Goldbach. Parmi ceux-ci, le résultat est que chaque entier pair supérieur à 2 est la somme d'au plus six nombres premiers (prouvé en 1995 par O. Ramaré) et que tout entier positif suffisamment grand est la somme d'un premier et un nombre premier ou le produit de deux nombres premiers (prouvé en 1966 par JR Chen). Peut-être que la conjecture de Goldbach sera réglée dans un avenir pas trop lointain. ▲

EXEMPLE 8 Il existe de nombreuses conjectures affirmant qu'il existe une infinité de nombres premiers de certaines formes. Une conjecture de ce genre est la conjecture qu'il existe une infinité de nombres premiers de la forme $n^2 + 1$, où n est un entier positif. Par exemple, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, et bientôt. Le meilleur résultat actuellement connu est qu'il existe une infinité de nombres entiers positifs n tels que $n^2 + 1$ est premier ou le produit d'au plus deux nombres premiers (prouvé par Henryk Iwaniec en 1973 en utilisant des techniques avancées de la théorie analytique des nombres, bien au-delà de la portée de ce livre). ▲

EXEMPLE 9 **La conjecture des nombres premiers jumeaux Les nombres premiers jumeaux** sont des paires de nombres premiers qui diffèrent par 2, tels que 3 et 5, 5 et 7, 11 et 13, 17 et 19, et 4967 et 4969. La conjecture du premier principe affirme que il y a une infinité de nombres premiers jumeaux. Le résultat le plus fort prouvé concernant les nombres premiers jumeaux est qu'il y a une infinité de paires p et $p + 2$, où p est premier et $p + 2$ est premier ou produit de deux nombres premiers (prouvé par JR Chen en 1966). Le record du monde pour les nombres premiers jumeaux, en date du mi-2011, se compose des nombres $65{,}516{,}468{,}355 \cdot 2^{333{,}333} \pm 1$, qui ont $100{,}355$ décimales chiffres. ▲

CHRISTIAN GOLDBACH (1690-1764) Christian Goldbach est né à Königsberg, en Prusse, la ville connue pour son célèbre pont problème (qui sera étudié dans la section 10.5). Il est devenu professeur de mathématiques à l'Académie de Saint-Pétersbourg en 1725. En 1728 Goldbach se rend à Moscou pour instruire le fils du tsar. Il est entré dans le monde de la politique quand, en 1742, il est devenu membre du personnel au ministère russe des Affaires étrangères. Goldbach est surtout connu pour sa correspondance avec d'éminents mathématiciens, y compris Euler et Bernoulli, pour ses fameuses conjectures en théorie des nombres et pour plusieurs contributions à l'analyse.

Les plus grands diviseurs communs et les plus petits multiples communs

Le plus grand entier qui divise les deux entiers est appelé le **plus grand diviseur commun** de ces entiers.

DÉFINITION 2 Soit a et b *des* entiers, pas tous les deux zéro. Le plus grand entier d tel que $d \mid a$ et $d \mid b$ est appelé le *plus grand diviseur commun* de a et b. Le plus grand diviseur commun de a et b est noté par pgcd (a, b).

Le plus grand diviseur commun de deux nombres entiers, et non tous deux nuls, existe parce que l'ensemble des communs les diviseurs de ces nombres entiers sont non vides et finis. Une façon de trouver le plus grand diviseur commun de deux entiers est de trouver tous les diviseurs communs positifs des deux entiers, puis de prendre la le plus grand diviseur. Cela se fait dans les exemples 10 et 11. Plus tard, une méthode plus efficace pour trouver les plus grands diviseurs communs seront donnés.

EXEMPLE 10 Quel est le plus grand commun diviseur de 24 et 36?

Solution: Les diviseurs communs positifs de 24 et 36 sont 1, 2, 3, 4, 6 et 12. Par conséquent, pgcd $(24, 36) = 12$. ▲

EXEMPLE 11 Quel est le plus grand commun diviseur de 17 et 22?

Solution: les nombres entiers 17 et 22 n'ont pas de diviseurs communs positifs autres que 1, de sorte que pgcd $(17, 22) = 1$. ▲

Parce qu'il est souvent important de spécifier que deux entiers n'ont pas de diviseur positif commun autre que 1, nous avons la définition 3.

DÉFINITION 3 Les entiers a et b sont *relativement premiers* si leur plus grand diviseur commun est 1.

EXEMPLE 12 Par l'exemple 11, il s'ensuit que les nombres entiers 17 et 22 sont relativement premiers, car pgcd $(17, 22) = 1$. ▲

Parce que nous devons souvent spécifier qu'il n'y a pas deux entiers dans un ensemble d'entiers ayant un commun diviseur positif supérieur à 1, on fait la Définition 4.

DÉFINITION 4 Les entiers $a_1, a_2, \ldots, a_n$ sont *relativement premiers par paire* si gcd $(a_i, a_j) = 1$ chaque fois que $1 \leq i < j \leq n$.

EXEMPLE 13 Déterminer si les nombres entiers 10, 17 et 21 sont relativement premiers par paires et si le les entiers 10, 19 et 24 sont deux à deux relativement premiers.

Solution: comme gcd $(10, 17) = 1$, gcd $(10, 21) = 1$ et gcd $(17, 21) = 1$, nous concluons que 10, 17 et 21 sont deux à deux relativement premiers.

Parce que pgcd $(10, 24) = 2 > 1$, nous voyons que 10, 19 et 24 ne sont pas relativement par paires premier. ▲

Une autre façon de trouver le plus grand diviseur commun de deux entiers positifs consiste à utiliser le premier factorisations de ces nombres entiers. Supposons que les factorisations premières des entiers positifs a et b sont

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

où chaque exposant est un entier non négatif, et où tous les nombres premiers se produisant dans le nombre premier la factorisation de a ou b est incluse dans les deux factorisations, avec zéro exposant si nécessaire. Alors gcd (a, b) est donné par

$$\text{pgcd}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

où $\min(x, y)$ représente le minimum des deux nombres x et y. Pour montrer que cette formule pour gcd (a, b) est valide, nous devons montrer que l'entier sur le côté droit divise à la fois a et b, et qu'aucun entier plus grand ne le fait aussi. Cet entier divise à la fois a et b, car la puissance de chaque nombre premier dans la factorisation ne dépasse pas la puissance de ce nombre premier dans la factorisation de a ou de b. De plus, aucun entier plus grand ne peut diviser à la fois a et b, car les exposants de les nombres premiers de cette factorisation ne peuvent pas être augmentés et aucun autre nombre premier ne peut être inclus.

EXEMPLE 14 Les facteurs premiers de 120 et 500 étant $120 = 2^3 \cdot 3 \cdot 5$ et $500 = 2^2 \cdot 5^3$, le plus grand diviseur commun est

$$\text{pgcd}(120, 500) = 2^{\min(3, 2)} 3^{\min(1, 0)} 5^{\min(1, 3)} = 2^2 3^0 5^1 = 20.$$ ▲

Les factorisations premières peuvent également être utilisées pour trouver le plus **petit commun multiple** de deux entiers.

DÉFINITION 5 Le *plus petit multiple commun* des entiers positifs a et b est le plus petit entier positif qui est divisible par a et b. Le plus petit commun multiple de a et b est noté lcm (a, b).

Le multiple le moins commun existe car l'ensemble des nombres entiers divisibles par a et b est non vide (comme ab appartient à cet ensemble, par exemple), et tout ensemble non vide d'entiers positifs a un moindre élément (par la propriété bien ordonnée, qui sera discutée dans la section 5.2). Supposons que les factorisations premières de a et b soient comme précédemment. Alors le multiple le moins commun de a et b est donné par

$$\text{ppcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

où $\max(x, y)$ désigne le maximum des deux nombres x et y. Cette formule est valable car un multiple commun de a et b a au moins $\max(a_i, b_i)$ facteurs de p_i dans sa factorisation première, et le multiple le moins commun n'a pas d'autres facteurs premiers que ceux de a et b.

EXEMPLE 15 Quel est le plus petit commun multiple de $2^3 3^5 7^2$ et $2^4 3^3$?

Solution: nous avons

$$\text{ppcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3, 4)} 3^{\max(5, 3)} 7^{\max(2, 0)} = 2^4 3^5 7^2.$$ ▲

Le théorème 5 donne la relation entre le plus grand diviseur commun et le moins commun multiple de deux entiers. Cela peut être prouvé en utilisant les formules que nous avons dérivées pour ces quantités. La preuve de ce théorème est laissée comme exercice 31.

THÉORÈME 5 Soit a et b des entiers positifs. alors

$$ab = \text{pgcd}(a, b) \cdot \text{ppcm}(a, b).$$

L'algorithme euclidien

Calcul du plus grand diviseur commun de deux entiers directement à partir des factorisations premières de ces nombres entiers est inefficace. La raison en est qu'il est long de trouver la factorisation tions. Nous donnerons une méthode plus efficace pour trouver le plus grand diviseur commun, appelé **Algorithme euclidien** . Cet algorithme est connu depuis l'Antiquité. Il porte le nom du le mathématicien grec ancien Euclide, qui a inclus une description de cet algorithme dans son livre *Les éléments* .

Avant de décrire l'algorithme euclidien, nous montrerons comment il est utilisé pour trouver gcd $(91, 287)$. Tout d'abord, divisez 287, le plus grand des deux nombres entiers, par 91, le plus petit, pour obtenir

$$287 = 91 \cdot 3 + 14.$$

Tout diviseur de 91 et 287 doit également être un diviseur de $287 - 91 \cdot 3 = 14$. De plus, tout diviseur de 91 et 14 doit aussi être un diviseur de $287 = 91 \cdot 3 + 14$. Par conséquent, le plus grand diviseur commun de 91 et 287 est le même que le plus grand diviseur commun de 91 et 14. Cela signifie que le problème de trouver un pgcd$(91, 287)$ a été réduit au problème de trouver un pgcd$(91, 14)$.

Ensuite, divisez 91 par 14 pour obtenir

$$91 = 14 \cdot 6 + 7.$$

Parce que tout diviseur commun de 91 et 14 divise également $91 - 14 \cdot 6 = 7$ et tout diviseur commun de 14 et 7 divise 91, il s'ensuit que pgcd$(91, 14)$ = pgcd$(14, 7)$.

Continuez en divisant 14 par 7, pour obtenir

$$14 = 7 \cdot 2.$$

Parce que 7 divise 14, il s'ensuit que pgcd (14, 7) = 7. De plus, parce que pgcd (287, 91) = gcd (91, 14) = gcd (14, 7) = 7, le problème d'origine a été résolu.

Nous décrivons maintenant comment l'algorithme euclidien fonctionne en général. Nous utiliserons successivement divisions pour réduire le problème de trouver le plus grand diviseur commun de deux entiers positifs au même problème avec des entiers plus petits, jusqu'à ce que l'un des entiers soit zéro.

L'algorithme euclidien est basé sur le résultat suivant sur les plus grands diviseurs communs et l'algorithme de division.

EUCLID (325 BCE - 265 BCE) Euclide était l'auteur du livre de mathématiques le plus réussi jamais écrit, *The Elements*, qui est apparu dans plus de 1000 éditions différentes de l'Antiquité aux temps modernes. On en sait peu sur la vie d'Euclide, autre que celle qu'il a enseignée à la célèbre académie d'Alexandrie en Egypte. Apparemment, Euclid n'a pas insisté sur les demandes. Quand un étudiant a demandé ce qu'il obtiendrait en apprenant la géométrie, Euclid a expliqué cette connaissance valait la peine d'être acquise pour lui-même et a dit à son serviteur de donner une pièce à l'étudiant «parce qu'il doit faire un profit de ce qu'il apprend. "

LEMMA 1 Soit $a = bq + r$, où a, b, q et r sont des entiers. Alors gcd (a, b) = gcd (b, r).

Preuve: si l'on peut montrer que les diviseurs communs de a et b sont les mêmes que les diviseurs communs de b et r, nous aurons montré que gcd (a, b) = gcd (b, r), car les deux paires doivent avoir le même *plus grand* diviseur commun.

Supposons donc que d divise à la fois a et b. Il s'ensuit que d divise également $a - bq = r$ (de Théorème 1 de la section 4.1). Par conséquent, tout diviseur commun de a et b est également un diviseur commun de b et r.

De même, supposons que d divise à la fois b et r. Alors d divise également $bq + r = a$. Par conséquent, tout le diviseur commun de b et r est aussi un diviseur commun de a et b.

Par conséquent, gcd (a, b) = gcd (b, r).

Supposons que a et b soient des entiers positifs avec $a \geq b$. Soit $r_0 = a$ et $r_1 = b$. quand nous appliquer successivement l'algorithme de division, on obtient

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2,\\
&\ \ \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_n .
\end{aligned}$$

Finalement, un reste de zéro se produit dans cette séquence de divisions successives, car le séquence de restes $a = r_0 > r_1 > r_2 > \cdots \geq 0$ ne peut pas contenir plus d' *un* terme. Fourrure- En outre, il ressort du lemme 1 que

$$\begin{aligned}
\text{pgcd}(a, b) &= \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2) = \cdots = \text{pgcd}(r_{n-2}, r_{n-1})\\
&= \text{pgcd}(r_{n-1}, r_n) = \text{pgcd}(r_n, 0) = r_n .
\end{aligned}$$

Par conséquent, le plus grand diviseur commun est le dernier reste non nul de la séquence de divisions.

EXEMPLE 16 Trouver le plus grand diviseur commun de 414 et 662 en utilisant l'algorithme euclidien.

Solution: Les utilisations successives de l'algorithme de division donnent:

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41 .$$

Par conséquent, pgcd (414, 662) = 2, car 2 est le dernier reste non nul. ▲

L'algorithme euclidien est exprimé en pseudocode dans l'algorithme 1.

ALGORITHME 1 L'algorithme euclidien.

procédure *gcd* (*a, b* : entiers positifs)
x : = *a*
y : = *b*
tandis que *y* = 0
  r : = *x* **mod** *y*
  x : = *y*
  y : = *r*
return *x* {gcd *(a, b)* is *x* }

Dans l'algorithme 1, les valeurs initiales de x et y sont respectivement a et b . À chaque étape de la , x est remplacé par y , et y est remplacé par x **mod** y , qui est le reste lorsque x est divisé par y . Ce processus est répété tant que $y = 0$. L'algorithme se termine lorsque $y = 0$, et la valeur de x à ce point, le dernier reste différent de zéro dans la procédure, est la plus grande diviseur commun de a et b .

Nous étudierons la complexité temporelle de l'algorithme euclidien dans la section 5.3, où nous montrera que le nombre de divisions nécessaires pour trouver le plus grand diviseur commun de a et b , où $a \geq b$, est O (log b).

gcds comme combinaisons linéaires

Un résultat important que nous utiliserons dans le reste de cette section est que le plus grand le diviseur commun de deux entiers a et b peut être exprimé sous la forme

$$sa + tb,$$

où s et t sont des entiers. En d'autres termes, le pgcd (a, b) peut être exprimé comme une **combinaison linéaire** avec des coefficients entiers de a et b . Par exemple, gcd $(6, 14) = 2$ et $2 = (-2) \cdot 6 + 1 \cdot 14$. Nous déclarons ce fait comme Théorème 6.

THÉORÈME 6 **THÉORÈME DE BÉZOUT** Si a et b sont des entiers positifs, alors il existe des entiers s et t tel que gcd $(a, b) = sa + tb$.

ÉTIENNE BÉZOUT (1730–1783) Bézout est né à Nemours, en France, où son père était magistrat. La lecture des écrits du grand mathématicien Leonhard Euler l'a incité à devenir mathématicien. Dans 1758, il est nommé à l'Académie des sciences de Paris; en 1763, il est nommé examinateur des Gardes de la Marine, où il a été chargé de rédiger des manuels de mathématiques. Cette mission conduit à un manuel en quatre volumes achevé en 1767. Bézout est bien connu pour ses six volumes complets manuel de mathématiques. Ses manuels étaient extrêmement populaires et ont été étudiés par de nombreuses générations de des étudiants souhaitant entrer à l'École Polytechnique, la célèbre école d'ingénieurs et de sciences. Ses livres étaient traduit en anglais et utilisé en Amérique du Nord, y compris à Harvard.

Son œuvre originale la plus importante a été publiée en 1779 dans le livre *Théorie générale des équations algébriques* , où il a introduit des méthodes importantes pour résoudre des équations polynomiales simultanées dans de nombreuses inconnues. Le plus Le résultat bien connu de ce livre est maintenant appelé *le théorème de Bézout* , qui dans sa forme générale nous dit que le nombre de points communs sur deux courbes algébriques planes sont égales au produit des degrés de ces courbes. Bézout est également crédité d'avoir inventé le déterminant (qui était appelé le Bézoutien par le grand mathématicien anglais James Joseph Sylvester) . Il était considéré comme une personne gentille avec un cœur chaleureux, bien qu'il ait eu une personnalité réservée et sombre. Il était marié et père de famille.

DÉFINITION 6 Si a et b sont des entiers positifs, alors les entiers s et t tels que gcd $(a, b) = sa + tb$ sont appelés *Coefficients* de *Bézout* de a et b (d'après Étienne Bézout, mathématicien français du XVIIIe siècle). De plus, l'équation gcd $(a, b) = sa + tb$ est appelée *identité de Bézout* .

Nous ne donnerons pas ici de preuve formelle du théorème 6 (voir exercice 36 dans la section 5.2 et [Ro10] pour les preuves). Nous fournirons un exemple de méthode générale qui peut être utilisée pour trouver un combinaison de deux entiers égaux à leur plus grand diviseur commun.(Dans cette section, nous allons supposons qu'une combinaison linéaire a des coefficients entiers.) La méthode procède en travaillant en arrière à travers les divisions de l'algorithme euclidien, donc cette méthode nécessite un avant passer et passer en arrière à travers les étapes de l'algorithme euclidien(Dans les exercices, nous décrira un algorithme appelé algorithme **euclidien étendu** , qui peut être utilisé pour exprimer gcd (a, b) comme une combinaison linéaire de a et b *en* utilisant un seul passage à travers les étapes de la Algorithme euclidien; voir le préambule de l'exercice 41.)

EXEMPLE 17 Exprimer le pgcd (252, 198) = 18 comme une combinaison linéaire de 252 et 198.

Solution: Pour montrer que gcd (252, 198) = 18, l'algorithme euclidien utilise ces divisions:

252 = 1 198 + 54
198 = 3, 54 + 36
54 = 1,36 + 18
36 = 2 · 18.

En utilisant l'avant-dernière division (la troisième division), nous pouvons exprimer gcd (252, 198) = 18 comme combinaison linéaire de 54 et 36. Nous constatons que

$$18 = 54 - 1 \cdot 36.$$

La deuxième division nous dit que

$$36 = 198\text{-}3,54 .$$

En substituant cette expression à 36 dans l'équation précédente, nous pouvons exprimer 18 comme linéaire combinaison de 54 et 198. Nous avons

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$

La première division nous dit que

$$54 = 252 - 1 \cdot 198 .$$

En substituant cette expression à 54 dans l'équation précédente, nous pouvons exprimer 18 comme linéaire combinaison de 252 et 198. Nous concluons que

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

compléter la solution. ▲

Nous utiliserons le théorème 6 pour développer plusieurs résultats utiles.L'un de nos objectifs sera de prouver la partie du théorème fondamental de l'arithmétique affirmant qu'un entier positif a au plus une factorisation principale. Nous montrerons que si un entier positif a une factorisation en nombres premiers, où les nombres premiers sont écrits dans un ordre non décroissant, alors cette factorisation est unique.

Premièrement, nous devons développer des résultats sur la divisibilité.

LEMMA 2 Si a , b et c sont des entiers positifs tels que gcd $(a, b) = 1$ et $a \mid bc$, puis $a \mid c$.

Preuve: Parce que gcd $(a, b) = 1$, par le théorème de Bézout il y a des entiers s et t tels que

$$sa + tb = 1 .$$

En multipliant les deux côtés de cette équation par c , nous obtenons

$$sac + tbc = c.$$

Nous pouvons maintenant utiliser le théorème 1 de la section 4.1 pour montrer que $un \mid c$. Par la partie (ii) de ce théorème, $un \mid$ *à confirmer* .
Parce *qu'un* $\mid sac$ et $un \mid tbc$, par la partie (i) de ce théorème, nous concluons que a divise $sac + tbc$.
Parce que $sac + tbc = c$, nous concluons que $a \mid c$, complétant la preuve.

Nous utiliserons la généralisation suivante du lemme 2 dans la preuve de l'unicité de prime factorisations. (La preuve du lemme 3 est conservée comme exercice 64 dans la section 5.1, car elle peut être le plus facilement réalisé en utilisant la méthode d'induction mathématique, décrite dans cette section.)

LEMMA 3 Si p est un nombre premier et $p \mid a_1 a_2 \cdots a_n$, où chaque a_i est un entier, alors $p \mid un_i$ pour certains i .

Nous pouvons maintenant montrer qu'une factorisation d'un entier en nombres premiers est unique.Autrement dit, nous allons montrent que chaque entier peut être écrit comme le produit de nombres premiers dans l'ordre non décroissant dans à la plupart d'une façon. Cela fait partie du théorème fondamental de l'arithmétique.Nous prouverons l'autre partie, que chaque entier a une factorisation en nombres premiers, dans la section 5.2.

Preuve (de l'unicité de la factorisation d'un nombre entier positif): Nous utiliserons un preuve par contradiction. Supposons que l'entier positif n puisse être écrit comme le produit de nombres premiers de deux manières différentes, disons $n = p_1 p_2 \cdots p_s$ et $n = q_1 q_2 \cdots q_t$, chaque p_i et q_j sont des nombres premiers tels que $p_1 \leq p_2 \leq \cdots \leq p_s$ et $q_1 \leq q_2 \leq \cdots \leq q_t$.

Lorsque nous supprimons tous les nombres premiers communs des deux factorisations, nous avons

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v},$$

où aucun nombre premier ne se produit des deux côtés de cette équation et u et v sont des entiers positifs. Par Lemme 3, il s'ensuit que p_{i_1} divise q_{j_k} pour certains k . Parce qu'aucun prime ne divise un autre premier, c'est impossible. Par conséquent, il peut y avoir au plus une factorisation de n en nombres premiers dans ordre non décroissant.

Le lemme 2 peut également être utilisé pour prouver un résultat sur la division des deux côtés d'une congruence par le même entier. Nous avons montré (Théorème 5 dans la section 4.1) que nous pouvons multiplier les deux côtés de une congruence par le même entier. Cependant, en divisant les deux côtés d'une congruence par un entier ne produit pas toujours une congruence valide, comme le montre l'exemple 18.

EXEMPLE 18 La congruence $14 \equiv 8 \pmod 6$ tient, mais les deux côtés de cette congruence ne peuvent pas être divisés par 2 pour produire une congruence valide car $14/2 = 7$ et $8/2 = 4$, mais $7 \not\equiv 4 \pmod 6$. ▲

Bien que nous ne pouvons pas diviser les deux côtés d'une congruence par un entier pour produire un valide congruence, nous pouvons si cet entier est relativement premier au module.Le théorème 7 établit ce fait important. Nous utilisons le lemme 2 dans la preuve.

THÉORÈME 7 Soit m un entier positif et a, b et c *des* entiers. Si $ac \equiv bc \pmod m$ et pgcd $(c, m) = 1$, puis $a \equiv b \pmod m$.

Preuve: Parce que $ac \equiv bc \pmod m$, $m \mid ac - bc = c(a - b)$. Par le lemme 2, car pgcd $(c, m) = 1$, il s'ensuit que $m \mid a - b$. Nous concluons que $a \equiv b \pmod m$.

Des exercices

1. Déterminez si chacun de ces nombres entiers est premier.

a) 21 **b)** 29
c) 71 **d)** 97
e) 111 **f)** 143

2. Déterminez si chacun de ces nombres entiers est premier.

a) 19 **b)** 27
c) 93 **d)** 101
e) 107 **f)** 113

3. Trouvez la factorisation en nombre premier de chacun de ces entiers.

a) 88 **b)** 126 **c)** 729
d) 1001 **e)** 1111 **f)** 909 090

4. Trouvez la décomposition en facteurs premiers de chacun de ces nombres entiers.

a) 39 **b)** 81 **c)** 101
d) 143 **e)** 289 **f)** 899

5. Trouvez la décomposition en facteurs premiers de 10 !.

∗ **6.** Combien de zéros y a-t-il à la fin de 100!?

7. Exprimer en pseudocode l'algorithme de division d'essai pour déterminer si un entier est premier.

8. Exprimez en pseudocode l'algorithme décrit dans le texte pour trouver la décomposition en facteurs premiers d'un entier.

9. Montrer que si *un* $^m + 1$ est composite si a et m sont des entiers supérieur à 1 et m est impair. [*Astuce:* Montrez que $x + 1$ est un facteur du polynôme $x^m + 1$ si m est impair.]

10. Montrez que si $2^m + 1$ est un nombre premier impair, alors $m = 2^n$ pour un entier non négatif n. [*Astuce:* montrer d'abord que l'identité polynomiale $x^m + 1 = (x^k + 1)(x^{k(t-1)} - x^{k(t-2)} + \cdots - x^k + 1)$ tient, où $m = kt$ et t est impair.]

∗ **11.** Montrez que le $\log_2 3$ est un nombre irrationnel. Rappelons qu'un ir- le nombre rationnel est un nombre réel x qui ne peut pas être écrit comme le rapport de deux entiers.

12. Montrer que pour tout entier positif n, il y a n con- entiers composites secutifs. [*Astuce:* Considérez le n con- entiers sécutifs commençant par $(n + 1)! + 2$.]

∗ **13.** Prouver ou infirmer qu'il y a trois impaires consécutifs entiers positifs qui sont des nombres premiers, c'est-à-dire des nombres premiers impairs de les formes p, $p + 2$ et $p + 4$.

14. Quels entiers positifs inférieurs à 12 sont premiers à 12?

15. Quels entiers positifs inférieurs à 30 sont relativement premiers à 30?

16. Déterminez si les nombres entiers dans chacun de ces ensembles sont par paire relativement premier.

a) 21, 34, 55 **b)** 14, 17, 85
c) 25, 41, 49, 64 **d)** 17, 18, 19, 23

17. Déterminez si les nombres entiers dans chacun de ces ensembles sont par paire relativement premier.

a) 11, 15, 19 **b)** 14, 15, 21
c) 12, 17, 31, 37 **d)** 7, 8, 9, 11

18. On appelle un entier positif **parfait** s'il est égal à la somme de ses diviseurs positifs autres que lui-même.

a) Montrez que 6 et 28 sont parfaits.
b) Montrer que $2^{p-1}(2^p - 1)$ est un nombre parfait lorsque $2^p - 1$ est premier.

19. Montrez que si $2^n - 1$ est premier, alors n est premier. [*Astuce:* utiliser l'identité $2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$.]

20. Déterminez si chacun de ces nombres entiers est premier, fying certaines des revendications de Mersenne.

a) $2^7 - 1$ **b)** $2^9 - 1$
c) $2^{11} - 1$ **d)** $2^{13} - 1$

La valeur de l' **Euler *de* la -fonction** à l'entier positif n est défini comme le nombre d'entiers positifs inférieur ou égal à n qui sont relativement premiers à n. [*Remarque:* φ est le grec lettre phi.]

21. Trouvez ces valeurs de la fonction Euler φ.

a) $\varphi(4)$. **b)** $\varphi(10)$. **c)** $\varphi(13)$.

22. Montrer que n est premier si et seulement si $\varphi(n) = n - 1$.

23. Quelle est la valeur de $\varphi(p^k)$ lorsque p est premier et k est un entier positif?

24. Quels sont les plus grands diviseurs communs de ces paires de des entiers?

a) $2^2 \cdot 3^3 \cdot 5^5$, $2^5 \cdot 3^3 \cdot 5^2$
b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17, 17^{17}$ **d)** $2^{2} \cdot 7, 5^{3} \cdot 13$
e) 0, 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$

25. Quels sont les plus grands diviseurs communs de ces paires de des entiers?

a) $3^{7} \cdot 5^{3} \cdot 7^{3}, 2^{11} \cdot 3^{5} \cdot 5^{9}$
b) $11 \cdot 13 \cdot 17, 2^{9} \cdot 3^{7} \cdot 5^{5} \cdot 7^{3}$
c) $23^{31}, 23^{17}$
d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$
e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$
f) 1111, 0

26. Quel est le multiple le moins commun de chaque paire dans Exercise 24?

27. Quel est le multiple le moins commun de chaque paire dans Exercise 25?

28. Trouvez gcd $(1000, 625)$ et lcm $(1000, 625)$ et vérifiez que pgcd $(1000, 625) \cdot$ ppcm $(1000, 625) = 1000 \cdot 625$.

29. Trouvez gcd (92928, 123552) et ppcm (92928, 123552), et vérifiez que pgcd (92928, 123552) · ppcm (92928, 123552) = 92928 · 123552. [*Astuce:* Trouvez d'abord les factorisations premières de 92928 et 123552.]

30. Si le produit de deux nombres entiers est $2^{7} 3^{8} 5^{2} 7^{11}$ et leur grand- le plus commun diviseur est $2^{3} 3^{4} 5$, quel est le moins commun plusieurs?

31. Montrer que si a et b sont des entiers positifs, alors $ab =$ pgcd $(a, b) \cdot$ ppcm (a, b). [*Astuce:* utilisez les factorisations principales de a et b et les formules pour pgcd (a, b) et lcm (a, b) en termes de ces factorisations.]

32. Utilisez l'algorithme euclidien pour trouver

a) pgcd $(1, 5)$. **b)** pgcd $(100, 101)$.
c) pgcd $(123, 277)$. **d)** pgcd $(1529, 14039)$.
e) pgcd $(1529, 14038)$. **f)** pgcd $(11111, 111111)$.

33. Utilisez l'algorithme euclidien pour trouver

a) pgcd $(12, 18)$. **b)** pgcd $(111, 201)$.
c) pgcd $(1001, 1331)$. **d)** pgcd $(12345, 54321)$.
e) pgcd $(1000, 5040)$. **f)** pgcd $(9888, 6060)$.

34. Combien de divisions sont nécessaires pour trouver le gcd $(21, 34)$ using l'algorithme euclidien?

35. Combien de divisions sont nécessaires pour trouver le pgcd $(34, 55)$ using l'algorithme euclidien?

∗ **36.** Montrez que si a et b sont tous deux des entiers positifs, alors $(2^{a} - 1) \bmod (2^{b} - 1) = 2^{a \bmod b} - 1$.

∗ **37.** Utilisez l'exercice 36 pour montrer que si a et b sont posi-

entiers positifs, puis pgcd $(2^{a} - 1, 2^{b} - 1) = 2^{\text{pgcd}(a, b)} - 1$. [*Indice:* montrez que les restes obtenus lors de la l'algorithme clidean est utilisé pour calculer gcd $(2^{a} - 1, 2^{b} - 1)$ sont de la forme $2^{r} - 1$, où r est un reste résultant lorsque l'algorithme euclidien est utilisé pour trouver gcd (a, b).]

38. Utilisez l'exercice 37 pour montrer que les nombres entiers $2^{35} - 1, 2^{34} - 1, 2^{33} - 1, 2^{31} - 1, 2^{29} - 1$ et $2^{23} - 1$ sont par paire relativement prime.

39. En utilisant la méthode suivie dans l'exemple 17, exprimez la le plus grand diviseur commun de chacune de ces paires d'entiers comme une combinaison linéaire de ces nombres entiers.

a) 10, 11 **b)** 21, 44 **c)** 36, 48
d) 34, 55 **e)** 117, 213 **f)** 0, 223
g) 123, 2347 **h)** 3454, 4666 **i)** 9999, 11111

40. En utilisant la méthode suivie dans l'exemple 17, exprimez la le plus grand diviseur commun de chacune de ces paires d'entiers comme une combinaison linéaire de ces nombres entiers.

a) 9, 11 **b)** 33, 44 **c)** 35, 78
d) 21, 55 **e)** 101, 203 **f)** 124, 323
g) 2002, 2339 **h)** 3457, 4669 **i)** 10001, 13422

L' **algorithme euclidien étendu** peut être utilisé pour exprimer pgcd (a, b) comme une combinaison linéaire avec des coefficients entiers de les entiers a et b. Nous fixons $s_0 = 1$, $s_1 = 0$, $t_0 = 0$ et $t_1 = 1$ et soit $s_j = s_{j-2} - q_{j-1} s_{j-1}$ et $t_j = t_{j-2} - q_{j-1} t_{j-1}$ pour $j = 2, 3, \ldots, n$, où les q_j sont les quotients dans le divisions utilisées lorsque l'algorithme euclidien trouve gcd (a, b), comme indiqué dans le texte. On peut montrer (voir [Ro10]) que pgcd $(a, b) = s_n a + t_n b$. Le principal avantage de l'extension L'algorithme euclidien est qu'il utilise un passage à travers les étapes de l'algorithme euclidien pour trouver les coefficients de Bézout d' *un* et b, contrairement à la méthode dans le texte qui utilise deux passes.

41. Utilisez l'algorithme euclidien étendu pour exprimer pgcd $(26, 91)$ comme une combinaison linéaire de 26 et 91.

42. Utilisez l'algorithme euclidien étendu pour exprimer pgcd $(252, 356)$ sous la forme d'une combinaison linéaire de 252 et 356.

43. Utilisez l'algorithme euclidien étendu pour exprimer pgcd $(144, 89)$ comme une combinaison linéaire de 144 et 89.

44. Utilisez l'algorithme euclidien étendu pour exprimer pgcd $(1001, 100001)$ comme une combinaison linéaire de 1001 et 100001.

45. Décrire l'algorithme euclidien étendu en utilisant des pseudocode.

46. Trouver le plus petit entier positif avec exactement n différents facteurs positifs lorsque n est

a) 3. **b)** 4. **c)** 5.
d) 6. **e)** 10.

47. Pouvez-vous trouver une formule ou une règle pour le n ème terme par rapport aux nombres premiers ou à la factorisation de sorte que les termes initiaux de la séquence aient ces valeurs?

a) 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, ...
b) 1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, ...
c) 1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, ...
d) 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, ...
e) 1, 2, 3, 3, 5, 5, 7, 7, 7, 7, 11, 11, 13, 13, ...
f) 1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, 223092870, ...

48. Pouvez-vous trouver une formule ou une règle pour le n ème terme par rapport aux nombres premiers ou à la factorisation de sorte que les termes initiaux de la séquence aient ces valeurs?

a) 2, 2, 3, 5, 5, 7, 7, 11, 11, 11, 11, 13, 13, ...
b) 0, 1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 6, 6, ...
c) 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, ...
d) 1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, ...
e) 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, ...
f) 4, 9, 25, 49, 121, 169, 289, 361, 529, 841, 961, 1369, ...

49. Démontrer que le produit de trois entiers consécutifs quelconques est divisible par 6.

50. Montrer que si a, b et m sont des entiers tels que $m \geq 2$ et $a \equiv b \pmod{m}$, puis gcd $(a, m) =$ gcd (b, m).

∗ **51.** Prouver ou infirmer que $n^{2} - 79n + 1601$ est premier lorsque-

toujours n est un entier positif.

52. Prouver ou infirmer que $p_1 p_2 \cdots p_n + 1$ est premier pour chaque entier positif n, où $p_1, p_2, \ldots, p_n$ sont les n petits- est des nombres premiers.

53. Montrer qu'il y a un entier composite dans chaque arithmétique

de la forme $4k + 3$, où k est un entier non négatif ger. [*Astuce:* Supposons qu'il n'y ait qu'un nombre fini ces nombres premiers $q_1, q_2, \ldots, q_n$, et considérons le nombre $4 q_1 q_2 \cdots q_n - 1$.]

∗ **56.** Démontrer que l'ensemble des nombres rationnels positifs est dénombrable

en créant une fonction qui attribue à un nombre rationnel ber p/q avec pgcd $(p, q) = 1$ le nombre de base 11 formé progression $ak + b$, $k = 1, 2, \ldots$ où a et b sont pos- entiers itifs.

54. Adapter la preuve dans le texte qu'il existe une infinité de nombres premiers pour prouver qu'il existe une infinité de nombres premiers de la forme $3k + 2$, où k est une intégrale non négative ger. [*Astuce:* Supposons qu'il n'y ait qu'un nombre fini ces nombres premiers $q_1, q_2, \ldots, q_n$, et considérons le nombre $3q_1q_2 \cdots q_n - 1$.]

55. Adapter la preuve dans le texte qu'il y a une infinité de nombres premiers pour prouver qu'il existe une infinité de nombres premiers

par la représentation décimale de p suivie de la base 11 chiffres A, qui correspond au nombre décimal 10, suivi de la représentation décimale de q.

∗ **57.** Démontrer que l'ensemble des nombres rationnels positifs est dénombrable en montrant que la fonction K est une correspondance biunivoque dence entre l'ensemble des nombres rationnels positifs et l'ensemble des entiers positifs si $K(m/n) = p_1^{2a_1} p_2^{2a_2} \cdots p_s^{2a_s} q_1^{2b_1-1} q_2^{2b_2-1} \cdots q_t^{2b_t-1}$, où pgcd $(m, n) = 1$ et les factorisations de puissance première de m et n sont $m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ et $n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}$.

Résolution des congruences

introduction

La résolution des congruences linéaires, qui ont la forme $ax \equiv b \pmod{m}$, est une tâche essentielle dans l'étude de la théorie des nombres et de ses applications, tout comme la résolution d'équations linéaires joue un rôle dans le calcul et l'algèbre linéaire. Pour résoudre les congruences linéaires, nous utilisons des inverses modulo m. Nous expliquons comment travailler en arrière à travers les étapes de l'algorithme euclidien pour trouver des inverses modulo m. Une fois que nous avons trouvé l'inverse d'*un* modulo m, nous résolvons la congruence $ax \equiv b \pmod{m}$ en multipliant les deux côtés de la congruence par cet inverse.

Des systèmes simultanés de congruence linéaire ont été étudiés depuis l'Antiquité. Pour Par exemple, le mathématicien chinois Sun-Tsu les a étudiés au premier siècle. Nous montrerons comment résoudre des systèmes de congruences linéaires modulo par paires modules relativement premiers. Le résultat nous allons prouver est appelé le théorème du reste chinois, et notre preuve donnera une méthode pour trouver toutes les solutions de tels systèmes de congruences. Nous montrerons également comment utiliser le chinois théorème du reste comme base pour effectuer l'arithmétique avec de grands nombres entiers.

Nous présenterons un résultat utile de Fermat, connu comme le petit théorème de Fermat, qui déclare que si p est premier et p ne divise pas *un*, puis *un* $^{p-1} \equiv 1 \pmod{p}$. Nous allons examiner l'inverse de cette affirmation, qui nous conduira au concept de pseudoprime. Un pseudoprime m à la base a est un entier composite m qui se fait passer pour un nombre premier en satisfaisant la congruence $a^{m-1} \equiv 1 \pmod{m}$. Nous donnerons également un exemple d'un nombre de Carmichael, qui est un entier composite c'est un pseudoprime à toutes les bases *un* relativement premier à lui.

Nous introduisons également la notion de logarithmes discrets, qui sont analogues aux logarithmes ordinaires rithms. Pour définir des logarithmes discrets, nous devons d'abord définir les racines primitives. Une racine primitive d'un premier p est un entier r tel que tout entier non divisible par p soit congru à une puissance de r modulo p. Si r est une racine primitive de p et $r^e \equiv a \pmod{p}$, alors e est le logarithme discret de a modulo p à la base r. Trouver des logarithmes discrets s'avère être un problème extrêmement difficile le lem en général. La difficulté de ce problème est à la base de la sécurité de nombreux cryptographiques systèmes.

Congruences linéaires

Une congruence de la forme

$$ax \equiv b \pmod{m},$$

où m est un entier positif, a et b sont des entiers et x est une variable, est appelé **linéaire congruence**. De telles congruences surviennent tout au long de la théorie des nombres et de ses applications.

Comment pouvons-nous résoudre l' *axe de* congruence linéaire $\equiv b \pmod{m}$, c'est-à-dire comment trouver tous des entiers x qui satisfont cette congruence? Une méthode que nous allons décrire utilise un entier a tel que $aa \equiv 1 \pmod{m}$, si un tel entier existe. Un tel entier a est dit être un **inverse** d' *un* modulo m. Le théorème 1 garantit qu'un inverse d' *un* modulo m existe chaque fois *que* a et m sont relativement premiers.

THÉORÈME 1 Si a et m sont des entiers relativement premiers et $m > 1$, alors l'inverse d' *un* modulo m existe. De plus, cet inverse est unique modulo m. (Autrement dit, il existe un entier positif unique a inférieur à m qui est l'inverse d' *un* modulo m et tout autre inverse d' *un* modulo m est congruente à *un* modulo m.)

Preuve: par le théorème 6 de la section 4.3, car gcd$(a, m) = 1$, il existe des entiers s et t tels cette

$$sa + tm = 1 .$$

Ceci implique que

$$sa + tm \equiv 1 \pmod{m}.$$

Parce que $tm \equiv 0 \pmod{m}$, il s'ensuit que

$$sa \equiv 1 \pmod{m}.$$

Par conséquent, s est l'inverse d'*un* modulo m . Que cet inverse est unique modulo m est laissé comme Exercice 7.

L'utilisation de l'inspection pour trouver l'inverse d'*un* modulo m est facile lorsque m est petit. Pour trouver cela inverse, nous recherchons un multiple de a qui dépasse un multiple de m par 1. Par exemple, pour trouver un inverse de 3 modulo 7, on peut trouver $j \cdot 3$ pour $j = 1, 2, \ldots, 6$, s'arrêtant quand on trouve un multiple de 3 qui est un de plus qu'un multiple de 7. Nous pouvons accélérer cette approche si nous notons que $2 \cdot 3 \equiv -1 \pmod{7}$. Cela signifie que $(-2) \cdot 3 \equiv 1 \pmod{7}$. Par conséquent, $5 \cdot 3 \equiv 1 \pmod{7}$, donc 5 est un inverse de 3 modulo 7.

Nous pouvons concevoir un algorithme plus efficace que la force brute pour trouver l'inverse d'*un* modulo m lorsque gcd $(a, m) = 1$ en utilisant les étapes de l'algorithme euclidien.En inversant ces étapes comme dans l'exemple 17 de la section 4.3, nous pouvons trouver une combinaison linéaire $sa + tm = 1$ où s et t sont des entiers. La réduction des deux côtés de cette équation modulo m nous dit que s est l'inverse de *un* modulo m . Nous illustrons cette procédure dans l'exemple 1.

EXEMPLE 1 Trouver un inverse de 3 modulo 7 en trouvant d'abord les coefficients de Bézout de 3 et 7. (Notez que nous avons déjà montré que 5 est un inverse de 3 modulo 7 par inspection.)

Solution: Parce que gcd $(3, 7) = 1$, le théorème 1 nous dit qu'il existe un inverse de 3 modulo 7.le L'algorithme euclidien se termine rapidement lorsqu'il est utilisé pour trouver le plus grand diviseur commun de 3 et 7:

$$7 = 2 \cdot 3 + 1 .$$

De cette équation, nous voyons que

$$-2 \cdot 3 + 1 \cdot 7 = 1 .$$

Cela montre que −2 et 1 sont des coefficients de Bézout de 3 et 7. Nous voyons que −2 est un inverse de 3 modulo 7. Notez que tout entier congru à −2 modulo 7 est également un inverse de 3, comme 5, -9, 12, etc. ▲

EXEMPLE 2 Trouver un inverse de 101 modulo 4620.

Solution: pour être complet, nous présentons toutes les étapes utilisées pour calculer l'inverse de 101 modulo 4620. (Seule la dernière étape va au-delà des méthodes développées dans la section 4.3 et illustrées dans l'exemple 17 dans cette section.) Tout d'abord, nous utilisons l'algorithme euclidien pour montrer que pgcd $(101, 4620) = 1$. Ensuite nous inverserons les étapes pour trouver les coefficients de Bézout a et b tels que $101a + 4620b = 1$. Il ensuite, a est un inverse de 101 modulo 4620. Les étapes utilisées par l'algorithme euclidien pour trouver gcd $(101, 4620)$ sont

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1{,}75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1, 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 .$$

Comme le dernier reste non nul est 1, nous savons que gcd $(101, 4620) = 1$. Nous pouvons maintenant trouver les coefficients de Bézout pour 101 et 4620 en remontant ces étapes, en exprimant pgcd $(101, 4620) = 1$ en termes de chaque paire de restes successifs. À chaque étape, nous éliminons le reste en l'exprimant comme une combinaison linéaire du diviseur et du dividende. On obtient

$$\begin{aligned}
1 &= 3 - 1 \cdot 2\\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3\\
&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23\\
&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26\\
&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75\\
&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101.
\end{aligned}$$

Que $-35 \cdot 4620 + 1601 \cdot 101 = 1$ nous indique que -35 et 1601 sont des coefficients de Bézout de 4620 et 101, et 1601 est un inverse de 101 modulo 4620. ▲

Une fois que nous avons l'inverse $\bar{a}$ d' *un* modulo m, nous pouvons résoudre la congruence $ax \equiv b \pmod{m}$ en multipliant les deux côtés de la congruence linéaire par $\bar{a}$, comme l'illustre l'exemple 3.

EXEMPLE 3 Quelles sont les solutions de la congruence linéaire $3x \equiv 4 \pmod 7$?

Solution: Par l'exemple 1, nous savons que -2 est l'inverse de 3 modulo 7. Multipliant les deux côtés de la congruence de -2 montre que

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7.$$

Parce que $-6 \equiv 1 \pmod 7$ et $-8 \equiv 6 \pmod 7$, il s'ensuit que si x est une solution, alors $x \equiv -8 \equiv 6 \pmod 7$.

Nous devons déterminer si chaque x avec $x \equiv 6 \pmod 7$ est une solution. Suppose que $x \equiv 6 \pmod 7$. Ensuite, par le théorème 5 de la section 4.1, il s'ensuit que

$$3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod 7,$$

ce qui montre que tous ces x satisfont la congruence. Nous concluons que les solutions au la congruence sont les entiers x tels que $x \equiv 6 \pmod 7$, à savoir $6, 13, 20, \ldots$ et $-1, -8, -15, \ldots$. ▲

Le théorème du reste chinois

Des systèmes de congruences linéaires apparaissent dans de nombreux contextes. Par exemple, comme nous le verrons plus loin, ils sont la base d'une méthode qui peut être utilisée pour effectuer l'arithmétique avec de grands nombres entiers. De tels systèmes peut même être trouvé comme des puzzles de mots dans les écrits des anciens mathématiciens chinois et hindous, tel que celui donné dans l'exemple 4.

EXEMPLE 4 Au premier siècle, le mathématicien chinois Sun-Tsu a demandé:

> Il y a certaines choses dont le nombre est inconnu. Lorsqu'il est divisé par 3, le reste est 2; lorsqu'il est divisé par 5, le reste est 3; et lorsqu'il est divisé par 7, le reste est 2. Que sera le nombre de choses?

Ce puzzle peut se traduire par la question suivante: Quelles sont les solutions du systèmes de congruences

$$\begin{aligned}
x &\equiv 2 \pmod 3,\\
x &\equiv 3 \pmod 5,\\
x &\equiv 2 \pmod 7 ?
\end{aligned}$$

Nous allons résoudre ce système, et avec lui le puzzle de Sun-Tsu, plus loin dans cette section. ▲

Le *théorème du reste chinois* , nommé d'après l'héritage chinois des problèmes impliquant systèmes de congruences linéaires, déclare que lorsque les modules d'un système de congruences linéaires sont par paires relativement premiers, il existe une solution unique du système modulo le produit de la modules.

THÉORÈME 2 **LE THÉORÈME DU RESTANT CHINOIS** Soit m_1, m_2, ..., m_n soit par paire relativement premiers entiers positifs supérieurs à un et a_1, a_2, ..., a_n entiers arbitraires. Ensuite, le système

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

a une solution unique modulo $m = m_1 m_2 \cdots m_n$. (Autrement dit, il existe une solution x avec $0 \leq x < m$, et toutes les autres solutions sont modulo m congrues à cette solution.)

Preuve: Pour établir ce théorème, nous devons montrer qu'une solution existe et qu'elle est unique modulo m . Nous montrerons qu'une solution existe en décrivant une manière de construire cette solution; montrant que la solution est unique modulo m est l' exercice 30.

Pour construire une solution simultanée, laissez d'abord

$$M_k = m / m_k$$

pour $k = 1, 2, ..., n$. Autrement dit, M_k est le produit des modules à l'exception de m_k . Parce que m_i et m_k n'ont pas de facteurs communs supérieurs à 1 lorsque $i = k$, il s'ensuit que pgcd $(m_k, M_k) = 1$. Conse- par conséquent, par le théorème 1, nous savons qu'il existe un entier y_k , un inverse de M_k modulo m_k , tel cette

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Pour construire une solution simultanée, formez la somme

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n .$$

Nous allons maintenant montrer que x est une solution simultanée. Tout d'abord, notez que parce que $M_j \equiv 0 \pmod{m_k}$ chaque fois que $j = k$, tous les termes sauf le k ème terme de cette somme sont congruents à 0 modulo m_k . Car $M_k y_k \equiv 1 \pmod{m_k}$ on voit que

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k},$$

pour $k = 1, 2, ..., n$. Nous avons montré que x est une solution simultanée aux n congruences.

L'exemple 5 illustre comment utiliser la construction donnée dans notre preuve du reste chinois théorème pour résoudre un système de congruences. Nous allons résoudre le système donné dans l'exemple 4, résultant dans le puzzle de Sun-Tsu.

EXEMPLE 5 Pour résoudre le système de congruences de l'exemple 4, supposons d'abord $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m / 3 = 35$, $M_2 = m / 5 = 21$, et $M_3 = m / 7 = 15$. On voit que 2 est l'inverse de $M_1 = 35$ modulo 3, parce que $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$; 1 est un inverse de $M_2 = 21$ modulo 5, car $21 \equiv 1 \pmod 5$; et 1 est un inverse de $M_3 = 15 \pmod 7$, car $15 \equiv 1 \pmod 7$. Les solutions pour ce système sont ceux x tels que

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$
$$= 233 \equiv 23 \pmod{105}.$$

Il s'ensuit que 23 est le plus petit entier positif qui est une solution simultanée.Nous concluons que 23 est le plus petit entier positif qui laisse un reste de 2 lorsqu'il est divisé par 3, un reste de 3 lorsqu'il est divisé par 5, et un reste de 2 lorsqu'il est divisé par 7. ▲

Bien que la construction du théorème 2 fournisse une méthode générale pour résoudre les systèmes de congruences linéaires avec des modules relativement premiers par paires, il peut être plus facile de résoudre un système en utilisant une méthode différente. L'exemple 6 illustre l'utilisation d'une méthode connue sous le nom **de substitution de retour** .

EXEMPLE 6 Utilisez la méthode de substitution arrière pour trouver tous les entiers x tels que $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$ et $x \equiv 3 \pmod 7$.

Solution: Par le théorème 4 de la section 4.1, la première congruence peut être réécrite comme une égalité, $x = 5t + 1$ où t est un entier. Substitution de cette expression pour x dans la deuxième congruence nous dit que

$$5t + 1 \equiv 2 \pmod 6,$$

qui peut être facilement résolu pour montrer que $t \equiv 5 \pmod 6$ (comme le lecteur devrait vérifier).En utilisant Le théorème 4 de la section 4.1 montre à nouveau que $t = 6u + 5$ où u est un entier. Remplacer ceci l'expression de t dans l'équation $x = 5t + 1$ nous indique que $x = 5(6u + 5) + 1 = 30u + 26$. Nous l'insérons dans la troisième équation pour obtenir

$$30u + 26 \equiv 3 \pmod 7.$$

Résoudre cette congruence nous dit que $u \equiv 6 \pmod 7$ (comme le lecteur devrait vérifier). Par conséquent, Theorem 4 dans la section 4.1 nous dit que $u = 7v + 6$ où v est un entier. Substituer cette expression pour u dans l'équation $x = 30u + 26$ nous dit que $x = 30(7v + 6) + 26 = 210u + 206$. Trans- en rapportant cela à une congruence, nous trouvons la solution aux congruences simultanées,

$$x \equiv 206 \pmod{210}.$$ ▲

Arithmétique des ordinateurs avec de grands entiers

Supposons que $m_1, m_2, \ldots, m_n$ sont des modules relativement premiers par paires et que m soit leur produit. Par le théorème du reste chinois, nous pouvons montrer (voir exercice 28) qu'un entier a avec $0 \le a < m$ peut être représenté uniquement par le n-tuple composé de ses restes lors de la division par m_i, $i = 1, 2, \ldots, n$. Autrement dit, nous pouvons représenter uniquement *un* par

$$(un \ \mathbf{mod}\ m_1, un \ \mathbf{mod}\ m_2, \ldots, un \ \mathbf{mod}\ m_n).$$

EXEMPLE 7 Quelles sont les paires utilisées pour représenter les entiers non négatifs inférieurs à 12 lorsqu'ils sont représentés ressenti par la paire ordonnée où le premier composant est le reste de l'entier sur division par 3 et la deuxième composante est le reste de l'entier lors de la division par 4?

Solution: Nous avons les représentations suivantes, obtenues en trouvant le reste de chaque entier lorsqu'il est divisé par 3 et par 4:

$0 = (0, 0)$ $4 = (1, 0)$ $8 = (2, 0)$
$1 = (1, 1)$ $5 = (2, 1)$ $9 = (0, 1)$
$2 = (2, 2)$ $6 = (0, 2)$ $10 = (1, 2)$
$3 = (0, 3)$ $7 = (1, 3)$ $11 = (2, 3).$ ▲

Pour effectuer l'arithmétique avec de grands entiers, nous sélectionnons les modules $m_1, m_2, ..., m_n$, où chaque m_i est un entier supérieur à 2, pgcd $(m_i, m_j) = 1$ chaque fois que $i = j$, et $m = m_1 m_2 \cdots m_n$ est supérieur que les résultats des opérations arithmétiques que nous voulons effectuer.

Une fois que nous avons sélectionné nos modules, nous effectuons des opérations arithmétiques avec de grands entiers par effectuer des opérations composant par composant sur les n -tuples représentant ces entiers en utilisant leur restes après division par m_i, $i = 1, 2, ..., n$. Une fois que nous avons calculé la valeur de chaque composante dans le résultat, on récupère sa valeur en résolvant un système de n congruences modulo m_i, $i = 1, 2, ..., n$. Cette méthode d'exécution de l'arithmétique avec de grands entiers a plusieurs valeurs fonctionnalités compatibles. Tout d'abord, il peut être utilisé pour effectuer une arithmétique avec des entiers plus grands que ce qui est normalement possible être effectuée sur un ordinateur. Deuxièmement, les calculs par rapport aux différents modules peuvent être fait en parallèle, accélérant l'arithmétique.

EXEMPLE 8 Supposons que l'exécution d'une arithmétique avec des entiers inférieurs à 100 sur un certain processeur soit plus rapide que de faire de l'arithmétique avec des entiers plus grands. Nous pouvons restreindre presque tous nos calculs à entiers inférieurs à 100 si nous représentons des entiers en utilisant leurs restes modulo par paire relativement des nombres premiers inférieurs à 100. Par exemple, nous pouvons utiliser les modules de 99, 98, 97 et 95. (Ces les entiers sont relativement premiers par paire, car aucun n'a un facteur commun supérieur à 1.)

Selon le théorème du reste chinois, tout entier non négatif inférieur à 99 · 98 · 97 · 95 = 89 403 930 peuvent être représentés uniquement par leurs restes lorsqu'ils sont divisés par ces quatre uli. Par exemple, nous représentons 123 684 comme (33, 8, 9, 89), car 123 684 **mod** 99 = 33; 123,684 **mod** 98 = 8; 123.684 **mod** 97 = 9; et 123 684 **mod** 95 = 89. De même, nous représentons 413 456 as (32, 92, 42, 16).

Pour trouver la somme de 123 684 et 413 456, nous travaillons avec ces 4-tuples au lieu de ces deux entiers directement. Nous ajoutons les 4 tuples dans le sens des composants et réduisons chaque composant avec respect au module approprié. Cela donne

$$
\begin{aligned}
(33, 8, 9, 89) + (32, 92, 42, 16) \\
&= (65 \mathbf{ mod } 99, 100 \mathbf{ mod } 98, 51 \mathbf{ mod } 97, 105 \mathbf{ mod } 95) \\
&= (65, 2, 51, 10).
\end{aligned}
$$

Pour trouver la somme, c'est-à-dire l'entier représenté par (65, 2, 51, 10), nous devons résoudre le système de congruences

$$
\begin{aligned}
x &\equiv 65 \pmod{99}, \\
x &\equiv 2 \pmod{98}, \\
x &\equiv 51 \pmod{97}, \\
x &\equiv 10 \pmod{95}.
\end{aligned}
$$

On peut montrer (voir exercice 53) que 537 140 est la solution non négative unique de cette système inférieur à 89 403 930. Par conséquent, 537 140 est la somme. Notez que ce n'est que lorsque nous doivent récupérer l'entier représenté par (65, 2, 51, 10) que nous devons faire avec l'arithmétique entiers supérieurs à 100. ▲

Particulièrement bons choix pour les modules pour l'arithmétique avec de grands entiers sont des ensembles d'entiers de le formulaire $2^k - 1$, où k est un entier positif, car il est facile de faire du modulo arithmétique binaire de tels nombres entiers, et parce qu'il est facile de trouver des ensembles de tels nombres entiers relativement premiers par paire. [La deuxième raison est une conséquence du fait que gcd$(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a, b)} - 1$, comme L'exercice 37 de la section 4.3 le montre.] Supposons, par exemple, que nous puissions faire de l'arithmétique avec des nombres entiers moins de 2^{35} facilement sur notre ordinateur, mais que travailler avec des entiers plus grands nécessite des procédures. Nous pouvons utiliser des modules relativement premiers par paires inférieurs à 2^{35} pour effectuer l'arithmétique avec des entiers aussi grands que leur produit. Par exemple, comme le montre l'exercice 38 de la section 4.3, les nombres entiers $2^{35} - 1$, $2^{34} - 1$, $2^{33} - 1$, $2^{31} - 1$, $2^{29} - 1$ et $2^{23} - 1$ sont deux à deux relativement premiers. Parce que le produit de ces six modules dépasse 2^{184}, nous pouvons effectuer l'arithmétique avec des nombres entiers jusqu'à 2^{184} (tant que les résultats ne dépassent pas ce nombre) en faisant du modulo arithmétique chacun de ces six modules, dont aucun ne dépasse 2^{35}.

Le petit théorème de Fermat

Le grand mathématicien français Pierre de Fermat a fait de nombreuses découvertes importantes en nombre théorie. L'un des plus utiles de ces états où p divise un^{p-1} - 1 chaque fois que p est premier et a est un entier non divisible par p . Fermat a annoncé ce résultat dans une lettre à l'un de ses correspondants. Cependant, il n'a pas inclus de preuve dans la lettre, déclarant qu'il craignait la preuve serait trop long. Bien que Fermat n'ait jamais publié de preuve de ce fait, il ne fait aucun doute que il savait le prouver, contrairement au résultat connu sous le nom de dernier théorème de FermatLe premier publié la preuve est créditée à Leonhard Euler.Nous énonçons maintenant ce théorème en termes de congruences.

THÉORÈME 3 **PETIT THÉORÈME DE FERMAT** Si p est premier et a est un entier non divisible par p , ensuite

$$a^{p-1} \equiv 1 \pmod{p}.$$

De plus, pour chaque entier a, nous avons

$$a^{p} \equiv a \pmod{p}.$$

Remarque: le petit théorème de Fermat nous dit que si $a \in \mathbf{Z}_p$, alors $a^{p-1} = 1$ dans $\mathbf{Z}_p$.

La preuve du théorème 3 est décrite dans l'exercice 19.

Le petit théorème de Fermat est extrêmement utile pour calculer les restes modulo p des grands puissances d'entiers, comme l'illustre l'exemple 9.

EXEMPLE 9 Trouver 7^{222} **mod** 11.

Solution: Nous pouvons utiliser le petit théorème de Fermat pour évaluer 7^{222} **mod** 11 plutôt que d'utiliser le jeûne algorithme d'exponentiation modulaire. Par le petit théorème de Fermat, nous savons que $7^{10} \equiv 1 \pmod{11}$, donc $(7^{10})^k \equiv 1 \pmod{11}$ pour chaque entier positif k . Pour profiter de cette dernière congruence, nous divisons l'exposant 222 par 10, constatant que $222 = 22 \cdot 10 + 2$. Nous voyons maintenant que

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22}\, 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Il s'ensuit que 7^{222} **mod** $11 = 5$. ▲

L'exemple 9 illustre comment nous pouvons utiliser le petit théorème de Fermat pour calculer a^n **mod** p , où p est premier et $p \mid a$. Tout d'abord, nous utilisons l'algorithme de division pour trouver le quotient q et le reste r lorsque n est divisé par $p - 1$, de sorte que $n = q(p-1) + r$ où $0 \le r < p - 1$. Il s'ensuit que $a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$. Par conséquent, pour trouver un^n **mod** p , nous avons seulement besoin calculer un^r **mod** p . Nous profiterons de cette simplification à plusieurs reprises dans notre étude de la théorie du nombre.

Pseudoprimes

Dans la section 4.2, nous avons montré qu'un entier n est premier lorsqu'il n'est pas divisible par un premier p avec $p \le \sqrt{n}$. Malheureusement, l'utilisation de ce critère pour montrer qu'un entier donné est premier est inefficace. Il faut que l'on trouve tous les nombres premiers ne dépassant pas $\sqrt{n}$ et que nous effectuons la division d'essai par chaque un tel nombre premier pour voir s'il divise n .

Existe-t-il des moyens plus efficaces pour déterminer si un entier est premier?Selon certains sources, les anciens mathématiciens chinois croyaient que n était un nombre premier impair si et seulement si

$$2^{n-1} \equiv 1 \pmod{n}.$$

Si cela était vrai, cela fournirait un test de primalité efficace.Pourquoi ont-ils cru cela
la congruence pourrait être utilisée pour déterminer si un entier $n > 2$ est premier? Tout d'abord, ils ont observé
que la congruence tient chaque fois que n est un nombre impair impair. Par exemple, 5 est premier et

$$2^{5-1} = 2^4 = 16 \equiv 1 \pmod 5.$$

Par le petit théorème de Fermat, nous savons que cette observation était correcte, c'est-à-dire $2^{n-1} \equiv 1 \pmod n$ chaque fois que n est un nombre premier impair. Deuxièmement, ils n'ont jamais trouvé un entier composite n pour que la congruence détient. Cependant, les anciens Chinois n'étaient que partiellement corrects. Ils avaient raison de penser que la congruence est valable chaque fois que n est premier, mais elles étaient incorrectes en concluant que n est nécessairement premier si la congruence est vraie.

Malheureusement, il existe des entiers composites n tels que $2^{n-1} \equiv 1 \pmod n$. Ces entiers sont appelés **pseudoprimes** à la base 2.

EXEMPLE 10 Le nombre entier 341 est un pseudoprime à la base 2 car il est composite $(341 = 11 \cdot 31)$ et comme L'exercice 37 montre

$$2^{340} \equiv 1 \pmod{341}.$$

▲

Nous pouvons utiliser un entier autre que 2 comme base lorsque nous étudions les pseudoprimes.

DÉFINITION 1 Soit b un entier positif. Si n est un entier positif composite, et $b^{n-1} \equiv 1 \pmod n$, alors n est appelé un *pseudoprime à la base b* .

Étant donné un entier positif n , déterminer si $2^{n-1} \equiv 1 \pmod n$ est un test utile qui fournit fournit des preuves quant à savoir si n est premier. En particulier, si n satisfait cette congruence, alors il est soit premier, soit pseudoprime à la base 2;si n ne satisfait pas cette congruence, il est composite. Nous pouvons effectuer des tests similaires en utilisant des bases b autres que 2 et obtenir plus de preuves quant à savoir si n est premier. Si n réussit tous ces tests, il est soit premier, soit pseudoprime pour tous les bases b *que* nous avons choisies. De plus, parmi les entiers positifs ne dépassant pas x , où x est un nombre réel positif, par rapport aux nombres premiers, il y a relativement peu de pseudoprimes au base b , où b est un entier positif. Par exemple, parmi les entiers positifs inférieurs à 10^{10} il y a 455 052 512 nombres premiers, mais seulement 14 884 pseudoprimes à la base 2. Malheureusement, nous

PIERRE DE FERMAT (1601–1665) Pierre de Fermat, l'un des mathématiciens les plus importants de la XVIIe siècle, était avocat de profession. Il est le mathématicien amateur le plus célèbre de l'histoire. Fermat publié peu de ses découvertes mathématiques. C'est à travers sa correspondance avec d'autres mathématiciens que nous connaissons son travail. Fermat a été l'un des inventeurs de la géométrie analytique et a développé certains des les idées fondamentales du calcul. Fermat, avec Pascal, a donné à la théorie des probabilités une base mathématique. Fermat a formulé ce qui était le problème non résolu le plus célèbre en mathématiques. Il a affirmé que l'équation $x^n + y^n = z^n$ n'a pas de solutions entières positives non triviales lorsque n est un entier supérieur à 2. Pour plus de 300 ans, aucune preuve (ou contre-exemple) n'a été trouvée. Dans sa copie des travaux du mathématicien grec ancien Diophantus, Fermat a écrit qu'il avait une preuve mais qu'elle ne rentrerait pas dans la marge. Parce que la première preuve, trouvé par Andrew Wiles en 1994, repose sur des mathématiques sophistiquées et modernes, la plupart des gens pensent que Fermat pensait qu'il avait une preuve, mais que la preuve était incorrecte. Cependant, il peut avoir tenté les autres de chercher une preuve, sans pouvoir en trouver une lui-même.

ne peut pas faire la distinction entre les nombres premiers et les pseudoprimes simplement en choisissant suffisamment de bases, car il existe des entiers composites n qui réussissent tous les tests avec des bases b telles que gcd $(b, n) = 1$.
Cela conduit à la définition 2.

DÉFINITION 2 Un entier composite n qui satisfait la congruence $b^{n-1} \equiv 1 \pmod n$ pour tous les entiers positifs b avec gcd $(b, n) = 1$ est appelé un *nombre de Carmichael* . (Ces numéros sont nommés d'après Robert Carmichael, qui les a étudiés au début du XXe siècle.)

EXEMPLE 11 L'entier 561 est un nombre de Carmichael. Pour voir cela, notons d'abord que le 561 est un cause $561 = 3 \cdot 11 \cdot 17$. Ensuite, notez que si gcd $(b, 561) = 1$, alors gcd $(b, 3)$ = gcd $(b, 11)$ = pgcd $(b, 17) = 1$.

En utilisant le petit théorème de Fermat, nous constatons que

$$b^2 \equiv 1 \pmod 3, \; b^{10} \equiv 1 \pmod{11} \text{ et } b^{16} \equiv 1 \pmod{17}.$$

Il s'ensuit que

$$b^{560} = (b^2)^{280} \equiv 1 \pmod 3,$$

$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$,
$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$.

Par l'exercice 29, il s'ensuit que $b^{560} \equiv 1 \pmod{561}$ pour tous les entiers positifs b avec pgcd $(b, 561) = 1$. Par conséquent, 561 est un nombre Carmichael. ▲

Bien qu'il existe une infinité de nombres de Carmichael, des tests plus délicats, décrits dans l'ensemble d'exercices, peut être conçu pour servir de base à une primauté probabiliste efficace tests. De tels tests peuvent être utilisés pour montrer rapidement qu'il est presque certainement le cas entier est premier. Plus précisément, si un entier n'est pas premier, alors la probabilité qu'il passe un série de tests est proche de 0. Nous allons décrire un tel test dans le chapitre 7 et discuter des notions de la théorie des probabilités sur laquelle s'appuie ce test.Ces tests de primalité probabilistes peuvent être utilisés, et sont utilisés pour trouver de grands nombres premiers extrêmement rapidement sur les ordinateurs.

Racines primitives et logarithmes discrets

Dans l'ensemble des nombres réels positifs, si $b > 1$, et $x = b^y$, nous disons que y est le logarithme de x à la base b . Ici, nous montrerons que nous pouvons également définir le concept de logarithmes modulo p de entiers positifs où p est un nombre premier. Avant de le faire, nous avons besoin d'une définition.

DÉFINITION 3 Une *racine primitive* modulo a prime p est un entier r dans $\mathbf{Z}_p$ tel que chaque élément non nul de $\mathbf{Z}_p$ est une puissance de r .

ROBERT DANIEL CARMICHAEL (1879–1967) Robert Daniel Carmichael est né en Alabama. Ici-reçu son diplôme de premier cycle du Lineville College en 1898 et son doctorat. en 1911 de Princeton. Carmichael a occupé des postes à l'Université de l'Indiana de 1911 à 1915 et à l'Université de l'Illinois de 1915 jusqu'en 1947. Carmichael était un chercheur actif dans une grande variété de domaines, y compris la théorie des nombres, analyse, équations différentielles, physique mathématique et théorie des groupes. Son doctorat. thèse, rédigée sous le direction de GD Birkhoff, est considérée comme la première contribution américaine significative au sujet de la équations.

EXEMPLE 12 Déterminer si 2 et 3 sont des racines primitives modulo 11.

Solution: Lorsque nous calculons les puissances de 2 dans $\mathbf{Z}_{11}$, nous obtenons $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$. Parce que chaque élément de $\mathbf{Z}_{11}$ est une puissance de 2, 2 est une racine primitive de 11.

Lorsque nous calculons les puissances de 3 modulo 11, nous obtenons $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$. Nous notons que ce modèle se répète lorsque nous calculons des puissances supérieures de 3. Parce que tous les éléments de $\mathbf{Z}_{11}$ sont des puissances de 3, nous concluons que 3 n'est pas une racine primitive de 11. ▲

Un fait important dans la théorie des nombres est qu'il existe un module racine primitif p pour chaque premier p . Nous renvoyons le lecteur à [Ro10] pour une preuve de ce fait.Supposons que p est premier et r est une racine primitive modulo p . Si a est un entier compris entre 1 et $p - 1$, c'est-à-dire un élément de $\mathbf{Z}_p$, nous sachez qu'il existe un exposant unique e tel que $r^e = a$ dans $\mathbf{Z}_p$, c'est-à-dire r^e **mod** $p = a$.

DÉFINITION 4 Supposons que p est un nombre premier, r est un modulo racine primitif p et a est un entier compris entre 1 et $p - 1$ inclus. Si r^e **mod** $p = a$ et $0 \leq e \leq p - 1$, on dit que e est le *logarithme discret* d' *un* modulo p à la base r et on écrit $\log_r a = e$ (où le premier p est compris).

EXEMPLE 13 Trouver les logarithmes discrets de 3 et 5 modulo 11 à la base 2.

Solution: Lorsque nous avons calculé les puissances de 2 modulo 11 dans l'exemple 12, nous avons constaté que $2^8 = 3$ et $2^4 = 5$ dans $\mathbf{Z}_{11}$. Par conséquent, les logarithmes discrets de 3 et 5 modulo 11 à la base 2 sont 8 et 4, respectivement. (Ce sont les puissances de 2 qui sont respectivement égales à 3 et 5 dans $\mathbf{Z}_{11}$.) Nous écrivons $\log_2 3 = 8$ et $\log_2 5 = 4$ (où le module 11 est compris et n'est pas explicitement noté dans le notation). ▲

Le logarithme discret
le problème est difficile!

Le **problème du logarithme discret** prend en entrée un premier p , une racine primitive r modulo p , et un entier positif $a \in \mathbf{Z}_p$; sa sortie est le logarithme discret d' *un* modulo p à la base r . Bien que ce problème puisse sembler moins difficile, il s'avère qu'aucun polynôme algorithme de temps est connu pour le résoudre.La difficulté de ce problème joue un rôle important dans la cryptographie, comme nous le verrons dans la section 4.6

Des exercices

1. Montrez que 15 est l'inverse de 7 modulo 26.

2. Montrez que 937 est l'inverse de 13 modulo 2436.

3. Par inspection (comme discuté avant l'exemple 1), trouvez un inverse de 4 modulo 9.

4. Par inspection (comme discuté avant l'exemple 1), trouvez un inverse de 2 modulo 17.

5. Trouvez l'inverse d' *un* modulo m pour chacune de ces paires d'entiers relativement premiers en utilisant la méthode suivie dans Exemple 2.

a) $a = 4$, $m = 9$
b) $a = 19$, $m = 141$
c) $a = 55$, $m = 89$
d) $a = 89$, $m = 232$

6. Trouvez l'inverse d' *un* modulo m pour chacune de ces paires d'entiers relativement premiers en utilisant la méthode suivie dans Exemple 2.

a) $a = 2$, $m = 17$
b) $a = 34$, $m = 89$
c) $a = 144$, $m = 233$
d) $a = 200$, $m = 1001$

∗ **7.** Montrer que si a et m sont des entiers positifs relativement premiers gers, alors l'inverse d' *un* modulo m est unique modulo m . [*Astuce:* Supposons qu'il existe deux solutions b et c de l' *axe de* congruence $\equiv 1 \pmod{m}$. Utilisez le théorème 7 de Section 4.3 pour montrer que $b \equiv c \pmod{m}$.]

8. Montrer qu'un inverse d' *un* modulo m , où a est un integer et $m > 2$ est un entier positif, n'existe pas si pgcd $(a, m) > 1$.

9. Résoudre la congruence $4x \equiv 5 \pmod{9}$ *en* utilisant l'inverse de 4 modules 9 trouvés dans la partie (a) de l'exercice 5.

10. Résoudre la congruence $2x \equiv 7 \pmod{17}$ *en* utilisant l'inverse de 2 modules 7 trouvés dans la partie (a) de l'exercice 6.

11. Résolvez chacune de ces congruences en utilisant les informations modulaires versets trouvés dans les parties (b), (c) et (d) de l'exercice 5.

a) $19x \equiv 4 \pmod{141}$
b) $55x \equiv 34 \pmod{89}$
c) $89x \equiv 2 \pmod{232}$

Épisode 306

12. Résolvez chacune de ces congruences en utilisant l'information modulaire versets trouvés dans les parties (b), (c) et (d) de l'exercice 6.

a) $34x \equiv 77 \pmod{89}$
b) $144x \equiv 4 \pmod{233}$
c) $200x \equiv 13 \pmod{1001}$

13. Trouver les solutions de la congruence $15x^2 + 19x \equiv 5$ (mod 11). [*Astuce:* montrer que la congruence est équivalente à la congruence $15x^2 + 19x + 6 \equiv 0$ (mod 11). Facteur le côté gauche de la congruence; montrer qu'une solution de la congruence quadratique est une solution de l'un des deux différentes congruences linéaires.]

14. Trouver les solutions de la congruence $12x^2 + 25x \equiv$ 10 (mod 11). [*Astuce:* montrer que la congruence est l'équivalence à la congruence $12x^2 + 25x + 12 \equiv 0$ (mod 11). Fac- pour le côté gauche de la congruence; montrer qu'un lution de la congruence quadratique est une solution de l'un des deux congruences linéaires différentes.]

∗ **15.** Montrer que si m est un entier supérieur à 1 et $ac \equiv bc \pmod{m}$, puis $a \equiv b \pmod{m / \text{pgcd}(c, m)}$.

16. a) Montrer que les entiers positifs inférieurs à 11, sauf 1 et 10, peuvent être divisés en paires d'entiers telles que chaque paire est constituée d'entiers inverses de chaque autre modulo 11.

b) Utilisez la partie (a) pour montrer que $10! \equiv -1 \pmod{11}$.

17. Montrer que si p est premier, les seules solutions de $x^2 \equiv 1 \pmod{p}$ sont des entiers x tels que $x \equiv 1 \pmod{p}$ ou $x \equiv -1 \pmod{p}$.

∗ **18. a)** généraliser le résultat dans la partie (a) de l'exercice 16; cette est, montrer que si p est un nombre premier, les entiers positifs moins que p , sauf 1 et p - 1, peut être divisé en $(p - 3)/2$ paires d'entiers telles que chaque paire se compose de gers qui sont inverses les uns des autres. [*Astuce:* utilisez le résultat de l'exercice 17.]

b) De la partie (a) conclure que $(p - 1)! \equiv -1 \pmod{p}$ chaque fois que p est premier. Ce résultat est connu sous le nom de **Wilson théorème** .

c) Que pouvons-nous conclure si n est un entier positif tel ça $(n - 1)! \equiv -1 \pmod{n}$?

∗ **19.** Cet exercice présente une preuve du petit théorème de Fermat.

a) Supposons que a n'est pas divisible par le nombre premier p. Spectacle qu'aucun des nombres entiers $1 \cdot a, 2 \cdot a, \ldots, (p - 1)a$ sont modulo congru p .

b) conclure de la partie a) que le produit de $1, 2, \ldots, p - 1$ est modulo congru p au produit UCT de $a, 2a, \ldots, (p - 1)a$. Utilisez ceci pour montrer que

$$(p - 1)! \equiv a^{p-1} (p - 1)! \pmod{p}.$$

c) Utilisez le théorème 7 de la section 4.3 pour montrer à partir de la partie (b) qui $a^{p-1} \equiv 1 \pmod{p}$ si $p \mid a$. [*Astuce:* utilisez le lemme 3

20. Utilisez la construction dans la preuve du reste chinois théorème pour trouver toutes les solutions au système de congruences $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{4}$ et $x \equiv 3 \pmod{5}$.

21. Utilisez la construction dans la preuve du reste chinois- der le théorème pour trouver toutes les solutions au système de ences $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, et $x \equiv 4 \pmod{11}$.

22. Résoudre le système de congruence $x \equiv 3$ (mod 6) et $x \equiv 4$ (mod 7) en utilisant la méthode de substitution arrière.

23. Résoudre le système de congruences de l'exercice 20 en utilisant le méthode de substitution arrière.

24. Résoudre le système de congruences de l'exercice 21 en utilisant le méthode de substitution arrière.

25. Écrivez en pseudocode un algorithme pour résoudre un système multilingue de congruences linéaires basé sur la construction dans la preuve du reste chinois théo- rem.

∗ **26.** Trouver toutes les solutions, le cas échéant, au système de congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$ et $x \equiv 8 \pmod{15}$.

∗ **27.** Trouver toutes les solutions, le cas échéant, au système de congruences $x \equiv 7 \pmod{9}$, $x \equiv 4 \pmod{12}$ et $x \equiv 16 \pmod{21}$.

28. Utilisez le théorème du reste chinois pour montrer qu'un entier a , avec $0 \leq a < m = m_1 m_2 \cdots m_n$, où le les entiers positifs $m_1, m_2, \ldots, m_n$ sont relativement par paires premier, peut être représenté uniquement par le n -tuple (*un* **mod** m_1 , *un* **mod** m_2 , ..., *un* **mod** m_n).

∗ **29.** Soit $m_1, m_2, \ldots, m_n$ des entiers relativement premiers par paire supérieur ou égal à 2. Montrer que si $a \equiv b \pmod{m_i}$ pour $i = 1, 2, \ldots, n$, alors $a \equiv b \pmod{m}$, où $m = m_1 m_2 \cdots m_n$. (Ce résultat sera utilisé dans l'exercice 30 pour prouver le théorème du reste chinois. Par conséquent, n'utilisez pas le théorème du reste chinois pour le prouver.)

∗ **30.** Compléter la preuve du théorème du reste chinois en montrant que la solution simultanée d'un système des congruences linéaires modulo par paires relativement premiers moduli est unique modulo le produit de ces modules. [*Astuce:* Supposons que x et y sont deux solutions simultanées tions. Montrez que $m_i \mid x - y$ pour tout i . À l'aide de l'exercice 29, conclure que $m = m_1 m_2 \cdots m_n \mid x - y$.]

31. Quels entiers laissent un reste de 1 lorsqu'ils sont divisés par 2 et laisser également un reste de 1 lorsqu'il est divisé par 3?

32. Quels entiers sont divisibles par 5 mais laissent un reste de 1 lorsqu'il est divisé par 3?

33. Utilisez le petit théorème de Fermat pour trouver 7^{121} **mod** 13.

34. Utilisez le petit théorème de Fermat pour trouver 23^{1002} **mod** 41.

35. Utilisez le petit théorème de Fermat pour montrer que si p est premier et $p \mid a$, puis un^{p-2} est l'inverse d' *un* modulo p .

36. Utilisez l'exercice 35 pour trouver un inverse de 5 modulo 41.

de la section 4.3 pour montrer que p ne se divise pas $(p-1)!$ puis utilisez le théorème 7 de la section 4.3. Alternativement, utiliser le théorème de Wilson de l'exercice 18 (b).]

d) Utilisez la partie (c) pour montrer que $a^p \equiv a \pmod{p}$ pour tous les tegers a.

37. a) Montrer que $2^{340} \equiv 1 \pmod{11}$ du petit théo- rem et notant que $2^{340} = (2^{10})^{34}$.

b) Montrer que $2^{340} \equiv 1 \pmod{31}$ *en* utilisant le fait que $2^{340} = (2^5)^{68} = 32^{68}$.

c) conclure des parties a) et b) que $2^{340} \equiv 1 \pmod{341}$.

38. a) Utiliser le petit théorème de Fermat pour calculer 3^{302} **mod** 5, 3^{302} **mod** 7, et 3^{302} **mod** 11.

b) Utilisez vos résultats de la partie (a) et les réponses chinoises théorème de mainder pour trouver 3^{302} **mod** 385. (Notez que $385 = 5 \cdot 7 \cdot 11$.)

39. a) Utiliser le petit théorème de Fermat pour calculer 5^{2003} **mod** 7, 5^{2003} **mod** 11, et 5^{2003} **mod** 13.

b) Utilisez vos résultats de la partie (a) et les réponses chinoises théorème de mainder pour trouver 5^{2003} **mod** 1001. (Notez que $1001 = 7 \cdot 11 \cdot 13$.)

40. Montrez à l'aide du petit théorème de Fermat que si n est un entier positif, puis 42 divise $n^7 - n$.

41. Montrer que si p est un nombre premier impair, alors chaque diviseur de Mersenne numéro $2^p - 1$ est de la forme $2kp + 1$, où k est un entier non négatif. [*Astuce:* Utilisez le petit thé de Fermat- orem et exercice 37 de la section 4.3.]

42. Utilisez l'exercice 41 pour déterminer si $M_{13} = 2^{13} - 1 = 8191$ et $M_{23} = 2^{23} - 1 = 8,388,607$ sont premiers.

43. Utilisez l'exercice 41 pour déterminer si $M_{11} = 2^{11} - 1 = 2047$ et $M_{17} = 2^{17} - 1 = 131,071$ sont premiers.

Soit n un entier positif et soit $n - 1 = 2^s t$, où s est a entier non négatif et t est un entier positif impair. Nous disons que n passe **le test de Miller pour la base *b*** si soit $b^t \equiv 1 \pmod{n}$ ou $b^{2^j t} \equiv -1 \pmod{n}$ pour certains j avec $0 \leq j \leq s - 1$. Il peut être montré (voir [Ro10]) qu'un entier composite n passe Test de Miller pour moins de $n/4$ bases b avec $1 < b < n$. UNE entier positif composite n qui passe le test de Miller au la base b est appelée un **pseudoprime fort à la base *b***.

∗ **44.** Montrer que si n est premier et b est un entier positif avec $n \mid b$, puis n passe le test de Miller à la base b.

45. Montrer que 2047 est un pseudoprime fort pour la base 2 par montrant qu'il passe le test de Miller à la base 2, mais est composite.

46. Montrez que 1729 est un nombre Carmichael.

47. Montrez que 2821 est un nombre Carmichael.

∗ **48.** Montrer que si $n = p_1 p_2 \cdots p_k$, où $p_1, p_2, \ldots, p_k$ sont des nombres premiers distincts qui satisfont $p_j - 1 \mid n - 1$ pour $j = 1, 2, \ldots, k$, alors n est un nombre de Carmichael.

49. a) Utilisez l'exercice 48 pour montrer que chaque entier de la forme $(6m + 1)(12m + 1)(18m + 1)$, où m est positif entier et $6m + 1$, $12m + 1$ et $18m + 1$ sont tous nombres premiers, est un nombre de Carmichael.

b) Utilisez la partie (a) pour montrer que 172 947 529 est un numéro Michael.

50. Trouvez l'entier non négatif a inférieur à 28 représenté par chacune de ces paires, où chaque paire représente (*un* **mod** 4, *un* **mod** 7).

a) (0, 0)	**b)** (1, 0)	**c)** (1, 1)
d) (2, 1)	**e)** (2, 2)	**f)** (0, 3)
g) (2, 0)	**h)** (3, 5)	**i)** (3, 6)

51. exprimer chaque nombre entier non négatif a moins de 15 en tant que paire (*un* **mod** 3, *un* **mod** 5).

52. Expliquez comment utiliser les paires trouvées dans l'exercice 51 pour ajoutez 4 et 7.

53. Résoudre le système de congruences qui se pose dans l'exemple 8.

54. Montrez que 2 est une racine primitive de 19.

55. Trouvez les logarithmes discrets de 5 et 6 au module de base 2 ulo 19.

56. Soit p un nombre premier impair et r une racine primitive de p. Montrer que si a et b sont des entiers positifs dans $\mathbf{Z}_p$, alors $\log_r(ab) \equiv \log_r a + \log_r b \pmod{p-1}$.

57. Écrivez un tableau de logarithmes discrets modulo 17 avec par rapport à la racine primitive 3.

Si m est un entier positif, l'entier a est un **résidu quadratique** de m si gcd $(a, m) = 1$ et la congruence $x^2 \equiv a \pmod{m}$ a une solution. En d'autres termes, un résidu quadratique de m est un entier relativement premier à m qui est un modèle carré parfait ulo m. Si a n'est pas un résidu quadratique de m et pgcd $(a, m) = 1$, on dit que c'est un **non - résidu quadratique** de m. Pour l'examen- ple, 2 est un résidu quadratique de 7 parce que pgcd $(2, 7) = 1$ et $3^2 \equiv 2 \pmod{7}$ et 3 est un non-résidu quadratique de 7 car pgcd $(3, 7) = 1$ et $x^2 \equiv 3 \pmod{7}$ n'a pas de solution.

58. Quels entiers sont des résidus quadratiques de 11?

59. Montrer que si p est un nombre premier impair et a est un entier non divisible par p, alors la congruence $x^2 \equiv a \pmod{p}$ a soit pas de solutions ou exactement deux solutions incongrues modulo p.

60. Montrer que si p est un nombre premier impair, alors il y a exactement $(p-1)/2$ résidus quadratiques de p parmi les nombres entiers $1, 2, \ldots, p-1$.

Si p est un nombre premier impair et a est un entier non divisible par p, le **Symbole de Legendre** $\left(\frac{une}{p}\right)$ est défini comme étant 1 si a est un quadratique résidu de p et -1 sinon.

61. Montrer que si p est un nombre premier impair et a et b sont des entiers avec $a \equiv b \pmod{p}$, alors

$$\left(\frac{une}{p}\right) = \left(\frac{b}{p}\right).$$

62. Prouver **le critère d'Euler** , qui stipule que si p est un impair premier et a est un entier positif non divisible par p, alors

$$\left(\frac{une}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

[*Astuce:* Si a est un résidu quadratique modulo p, appliquez Fer- petit théorème de mat; sinon, appliquez le théorème de Wilson, donnée dans l'exercice 18 (b).]

63. Utiliser l' exercice 62 pour montrer que si p est un premier et bizarre *un* et b sont des entiers non divisibles par p, alors

$$\left(\frac{un\ B}{p}\right) = \left(\frac{une}{p}\right)\left(\frac{b}{p}\right).$$

64. Montrer que si p est un nombre premier impair, alors -1 est un quadratique résidu de p si $p \equiv 1 \pmod{4}$, et -1 n'est pas un quadratique résidu de p si $p \equiv 3 \pmod{4}$. [*Astuce:* utilisez l'exercice 62.]

65. Trouver toutes les solutions de la congruence $x^2 \equiv 29 \pmod{35}$. [*Astuce:* Trouvez les solutions de cette congruence modulo 5 et modulo 7, puis utilisez le théorème du reste chinois.]

66. Trouver toutes les solutions de la congruence $x^2 \equiv 16 \pmod{105}$.
[*Astuce:* Trouvez les solutions de cette congruence modulo 3, modulo 5 et modulo 7, puis utilisez le chinois théorème de Mainder.]

67. Décrire un algorithme de force brute pour résoudre le discret problème de logarithme et trouver le pire des cas et la moyenne complexité du temps de cas de cet algorithme.

Applications des congruences

Les congruences ont de nombreuses applications aux mathématiques discrètes, à l'informatique et à d'autres disciplines. Nous allons introduire trois applications dans cette section: l'utilisation des congruences pour attribuer des emplacements de mémoire aux fichiers informatiques, la génération de nombres pseudo-aléatoires, et vérifier les chiffres.

Supposons qu'un numéro d'identification client comporte dix chiffres. Pour récupérer les fichiers clients rapidement, nous ne voulons pas attribuer un emplacement de mémoire à un enregistrement client en utilisant les dix chiffres numéro d'identification. Au lieu de cela, nous voulons utiliser un plus petit entier associé à l'identification nombre. Cela peut être fait en utilisant ce que l'on appelle une fonction de hachage.Dans cette section, nous allons montrer comment nous pouvons utiliser l'arithmétique modulaire pour faire du hachage.

La construction de séquences de nombres aléatoires est importante pour les algorithmes randomisés, par simulations, et à de nombreuses autres fins. Construire une séquence de nombres vraiment aléatoires est extrêmement difficile, voire impossible, parce que toute méthode pour générer ce qui est supposé être des nombres aléatoires peut générer des nombres avec des motifs cachés.En conséquence, les méthodes ont été développés pour trouver des séquences de nombres qui ont de nombreuses propriétés souhaitables de des nombres aléatoires, et qui peuvent être utilisés à diverses fins à la place de nombres aléatoires. Dans cette section, nous montrerons comment utiliser les congruences pour générer des séquences de pseudo-aléatoire Nombres. L'avantage est que les nombres pseudo-aléatoires ainsi générés sont construits rapidement; l'inconvénient est qu'ils ont trop de prévisibilité pour être utilisés pour de nombreuses tâches.

Les congruences peuvent également être utilisées pour produire des chiffres de contrôle pour les numéros d'identification de divers types, tels que les numéros de code utilisés pour identifier les produits au détail, les numéros utilisés pour identifier les livres, numéros de billets d'avion, etc. Nous expliquerons comment construire des chiffres de contrôle en utilisant pour une variété de types de numéros d'identification.Nous montrerons que ces chiffres de contrôle peuvent être utilisé pour détecter certains types d'erreurs courantes commises lors de l'impression des numéros d'identification.

Fonctions de hachage

L'ordinateur central d'une compagnie d'assurance tient des registres pour chacun de ses clients. Comment attribuer des emplacements de mémoire afin que les enregistrements des clients puissent être récupérés rapidement?Le la solution à ce problème consiste à utiliser une **fonction de hachage** convenablement choisie . Les enregistrements sont identifiés à l'aide d'une **clé** , qui identifie de manière unique les enregistrements de chaque client.Par exemple, les enregistrements clients sont souvent identifiés en utilisant le numéro de sécurité sociale du client comme clé.Un hachage La fonction h affecte l'emplacement mémoire $h(k)$ à l'enregistrement qui a k comme clé.

En pratique, de nombreuses fonctions de hachage différentes sont utilisées. L'un des plus courants est le une fonction

$$h(k) = k \textbf{ mod } m$$

où m est le nombre d'emplacements de mémoire disponibles.

Les fonctions de hachage doivent être facilement évaluées afin que les fichiers puissent être rapidement localisés.Le la fonction de hachage $h(k) = k$ **mod** m répond à cette exigence; pour trouver $h(k)$, il suffit de calculer le reste lorsque k est divisé par m . En outre, la fonction de hachage doit être activée, de sorte que tous les emplacements de mémoire sont possibles. La fonction $h(k) = k$ **mod** m satisfait également cette propriété.

EXEMPLE 1 Trouver les emplacements mémoire attribués par la fonction de hachage $h(k) = k$ **mod** 111 aux enregistrements des clients avec les numéros de sécurité sociale 064212848 et 037149212.

Lösung: L'enregistrement du client avec le numéro de sécurité sociale 064212848 est assigné à emplacement mémoire 14, car

$$h(064212848) = 064212848 \textbf{ mod } 111 = 14.$$

De même, parce que

$$h(037149212) = 037149212 \textbf{ mod } 111 = 65,$$

l'enregistrement du client avec le numéro de sécurité sociale 037149212 est affecté à la mémoire emplacement 65. ▲

Parce qu'une fonction de hachage n'est pas un-à-un (car il y a plus de clés possibles que emplacements mémoire), plusieurs fichiers peuvent être affectés à un emplacement mémoire.Quand cela arrive, nous disons qu'une **collision** se produit. Une façon de résoudre une collision consiste à attribuer le premier emplacement libre suivant l'emplacement de mémoire occupé attribué par la fonction de hachage.

EXEMPLE 2 Après avoir affecté les enregistrements aux emplacements de mémoire de l'exemple 1, attribuez une mémoire emplacement à l'enregistrement du client avec le numéro de sécurité sociale 107405723.

Solution: notez d'abord que la fonction de hachage $h(k) = k$ **mod** 111 mappe la sécurité sociale numéro 107405723 à l'emplacement 14, car

$$h(107405723) = 107405723 \textbf{ mod } 111 = 14.$$

Cependant, cet emplacement est déjà occupé (par le dossier du client auprès de la Sécurité sociale numéro 064212848). Mais, parce que l'emplacement de mémoire 15, le premier emplacement après la mémoire l'emplacement 14, est gratuit, nous attribuons le dossier du client avec le numéro de sécurité sociale 107405723 à cet endroit. ▲

Dans l'exemple 1, nous avons utilisé une **fonction de sondage linéaire** , à savoir $h(k, i) = h(k) + i$ **mod** m , pour recherchez le premier emplacement de mémoire libre, où*je* passe de 0 à m - 1. Il existe de nombreux autres façons de résoudre les collisions qui sont discutées dans les références sur les fonctions de hachage données à la fin du livre.

Numéros pseudo-aléatoires

Des nombres choisis au hasard sont souvent nécessaires pour les simulations informatiques.Différentes méthodes ont été conçu pour générer des nombres qui ont des propriétés de nombres choisis au hasard.Car les nombres générés par des méthodes systématiques ne sont pas vraiment aléatoires, ils sont appelés**pseudo-aléatoires chiffres** .

La procédure la plus couramment utilisée pour générer des nombres pseudo-aléatoires est la **méthode congruentielle linéaire** . On choisit quatre entiers: le**module** m , le **multiplicateur** a , **incrément** c et **graine** x_0 , avec $2 \leq a < m$, $0 \leq c < m$ et $0 \leq x_0 < m$. Nous générons un de nombres pseudo-aléatoires $\{x_n\}$, avec $0 \leq x_n < m$ pour tout n , en utilisant successivement le fonction définie récursivement

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

(Ceci est un exemple de définition récursive, discuté à la section 5.3. Dans cette section, nous allons montrent que de telles séquences sont bien définies.)

De nombreuses expériences informatiques nécessitent la génération de nombres pseudo-aléatoires entre 0 et 1. Pour générer de tels nombres, nous divisons les nombres générés avec une congruentielle linéaire générateur par le module: c'est-à-dire que nous utilisons les nombres x_n / m .

EXEMPLE 3 Trouver la séquence de nombres pseudo-aléatoires générés par la méthode congruentielle linéaire avec module $m = 9$, multiplicateur $a = 7$, incrément $c = 4$ et germe $x_0 = 3$.

Solution: Nous calculons les termes de cette séquence en utilisant successivement la définition récursive fonction $x_{n+1} = (7x_n + 4) \mathbf{mod}\ 9$, en commençant par insérer la graine $x_0 = 3$ pour trouver x_1 . Nous trouvons cette

$$x_1 = 7x_0 + 4 \mathbf{mod}\ 9 = 7 \cdot 3 + 4 \mathbf{mod}\ 9 = 25 \mathbf{mod}\ 9 = 7,$$
$$x_2 = 7x_1 + 4 \mathbf{mod}\ 9 = 7 \cdot 7 + 4 \mathbf{mod}\ 9 = 53 \mathbf{mod}\ 9 = 8,$$
$$x_3 = 7x_2 + 4 \mathbf{mod}\ 9 = 7 \cdot 8 + 4 \mathbf{mod}\ 9 = 60 \mathbf{mod}\ 9 = 6,$$
$$x_4 = 7x_3 + 4 \mathbf{mod}\ 9 = 7 \cdot 6 + 4 \mathbf{mod}\ 9 = 46 \mathbf{mod}\ 9 = 1,$$
$$x_5 = 7x_4 + 4 \mathbf{mod}\ 9 = 7 \cdot 1 + 4 \mathbf{mod}\ 9 = 11 \mathbf{mod}\ 9 = 2,$$
$$x_6 = 7x_5 + 4 \mathbf{mod}\ 9 = 7 \cdot 2 + 4 \mathbf{mod}\ 9 = 18 \mathbf{mod}\ 9 = 0,$$
$$x_7 = 7x_6 + 4 \mathbf{mod}\ 9 = 7 \cdot 0 + 4 \mathbf{mod}\ 9 = 4 \mathbf{mod}\ 9 = 4,$$
$$x_8 = 7x_7 + 4 \mathbf{mod}\ 9 = 7 \cdot 4 + 4 \mathbf{mod}\ 9 = 32 \mathbf{mod}\ 9 = 5,$$
$$x_9 = 7x_8 + 4 \mathbf{mod}\ 9 = 7 \cdot 5 + 4 \mathbf{mod}\ 9 = 39 \mathbf{mod}\ 9 = 3.$$

Parce que $x_9 = x_0$ et parce que chaque terme ne dépend que du terme précédent, nous voyons que le séquence

$$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$$

est généré. Cette séquence contient neuf nombres différents avant de se répéter. ▲

La plupart des ordinateurs utilisent des générateurs congruentiels linéaires pour générer des nombres pseudo-aléatoires. Souvent, un générateur congruentiel linéaire avec incrément $c = 0$ est utilisé. Un tel générateur est appelé un **générateur multiplicatif pur** . Par exemple, le générateur multiplicatif pur avec module $2^{31} - 1$ et multiplicateur $7^5 = 16,807$ est largement utilisé. Avec ces valeurs, on peut montrer que $2^{31} - 2$ nombres sont générés avant le début de la répétition.

Les nombres pseudo-aléatoires générés par des générateurs linéaires congruents sont utilisés depuis longtemps pour de nombreuses tâches. Malheureusement, il a été démontré que des séquences de nombres pseudo-aléatoires de cette manière ne partagent pas certaines propriétés statistiques importantes que les vrais nombres aléatoires avoir. Pour cette raison, il n'est pas conseillé de les utiliser pour certaines tâches, telles que les grandes simulations. Pour de telles tâches sensibles, d'autres méthodes sont utilisées pour produire des séquences de nombres pseudo-aléatoires. bers, soit en utilisant une sorte d'algorithme ou des nombres d'échantillonnage résultant d'un physique aléatoire phénomène. Pour plus de détails sur le nombre pseudo-aléatoire, voir [Kn97] et [Re10].

Vérifier les chiffres

Les congruences sont utilisées pour vérifier les erreurs dans les chaînes de chiffres. Une technique courante pour détecter erreurs dans de telles chaînes est d'ajouter un chiffre supplémentaire à la fin de la chaîneCe dernier chiffre, ou chiffre de contrôle, est calculé à l'aide d'une fonction particulière. Ensuite, pour déterminer si une chaîne de chiffres est correcte, un une vérification est effectuée pour voir si ce dernier chiffre a la valeur correcte. Nous commençons par une application de cette idée pour vérifier l'exactitude des chaînes de bits.

EXEMPLE 4 **Bits de contrôle de parité** Les informations numériques sont représentées par une chaîne de bits, divisée en blocs d'un taille spécifiée. Avant que chaque bloc ne soit stocké ou transmis, un bit supplémentaire, appelé **bit de contrôle de parité** , peut être ajouté à chaque bloc. Le bit de contrôle de parité x_{n+1} pour la chaîne de bits $x_1 x_2 \ldots x_n$ est défini par

$x_{n+1} = x_1 + x_2 + \cdots + x_n$ **mod** 2 .

Il s'ensuit que x_{n+1} vaut 0 s'il y a un nombre pair de 1 bits dans le bloc de n bits et il vaut 1 si il y a un nombre impair de 1 bits dans le bloc de n bits. Lorsque nous examinons une chaîne qui comprend un bit de contrôle de parité, nous savons qu'il contient une erreur si le bit de contrôle de parité est incorrect.cependant, lorsque le bit de contrôle de parité est correct, il peut toujours y avoir une erreur.Un contrôle de parité peut détecter un impair nombre d'erreurs dans les bits précédents, mais pas un nombre pair d'erreurs.(Voir l'exercice 14.)

Supposons que nous recevions dans une transmission les chaînes de bits 01100101 et 11010110, chacune se terminant avec un bit de contrôle de parité. Devrions-nous accepter ces chaînes de bits comme correctes?

Solution: Avant d'accepter ces chaînes comme correctes, nous examinons leurs bits de contrôle de parité.le le bit de contrôle de parité de la première chaîne est 1. Parce que 0 + 1 + 1 + 0 + 0 + 1 + 0 ≡ 1 (mod 2), le le bit de contrôle de parité est correct.Le bit de contrôle de parité de la deuxième chaîne est 0. Nous constatons que 1 + 1 + 0 + 1 + 0 + 1 + 1 ≡ 1 (mod 2), donc le contrôle de parité est incorrect.Nous concluons que le premier la chaîne peut avoir été transmise correctement et nous savons avec certitude que la deuxième chaîne était transmis de manière incorrecte. Nous acceptons la première chaîne comme correcte (même si elle peut encore contenir un nombre pair d'erreurs), mais nous rejetons la deuxième chaîne. ▲

Les bits de contrôle calculés à l'aide de congruences sont largement utilisés pour vérifier l'exactitude de divers types de numéros d'identification. Les exemples 5 et 6 montrent comment les bits de contrôle sont calculés pour les codes qui identifient les produits (Universal Product Codes) et les livres (International Standard Numéros de livre). Les préambules des exercices 18, 28 et 32 présentent l'utilisation des congruences pour rechercher et utiliser des chiffres de chèque dans les numéros de mandat, les numéros de billet d'avion et l'identification les numéros des périodiques, respectivement. Notez que les congruences sont également utilisées pour calculer la vérification chiffres pour les numéros de compte bancaire, les numéros de permis de conduire, les numéros de carte de crédit et bien d'autres types de numéros d'identification.

EXEMPLE 5 CUP Les produits **vendus au** détail sont identifiés par leur **code produit universel (CUP)** . Le plus la forme courante d'un CUP comporte 12 chiffres décimaux: le premier chiffre identifie la catégorie de produit, le les cinq chiffres suivants identifient le fabricant, les cinq suivants identifient le produit particulier, et le dernier chiffre est un chiffre de contrôle. Le chiffre de contrôle est déterminé par la congruence

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \ (\text{mod } 10).$$

Répondez à ces questions:

(a) Supposons que les 11 premiers chiffres d'un CUP soient 79357343104. Quel est le chiffre de contrôle?
(b) 041331021641 est-il un CUP valide?

Solution: (a) Nous insérons les chiffres de 79357343104 dans la congruence pour UPC vérifier les chiffres. Cela donne $3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \ (\text{mod } 10)$. Pour simplifier, nous avons $21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \ (\text{mod } 10)$. Par conséquent, $98 + x_{12} \equiv 0 \ (\text{mod } 10)$. Il s'ensuit que $x_{12} \equiv 2 \ (\text{mod } 10)$, donc le le chiffre de contrôle est 2.

(b) Pour vérifier si 041331021641 est valide, nous insérons les chiffres dans la congruence de ces chiffres doit satisfaire. Cela donne $3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + 1 \equiv 0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 \equiv 4 \not\equiv 0 (\text{mod } 10)$. Par conséquent, 041331021641 n'est pas un UPC valide. ▲

EXEMPLE 6 ISBN Tous les livres sont identifiés par un **numéro international normalisé de livre (ISBN-10)**, un Code à 10 chiffres $x_1 x_2 \ldots x_{10}$, attribué par l'éditeur. (Récemment, un code à 13 chiffres appelé ISBN-13 a été introduit pour identifier un plus grand nombre d'ouvrages publiés; voir le préambule de l'exercice 42 dans les exercices supplémentaires.) Un ISBN-10 se compose de blocs identifiant la langue, l'éditeur, le numéro attribué au livre par sa maison d'édition et enfin un chèque chiffre qui est soit un chiffre soit la lettre X (utilisé pour représenter 10). Ce chiffre de contrôle est sélectionné afin cette

N'oubliez pas que le chèque chiffre d'un ISBN-10 peut être un X!

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \ (\text{mod } 11),$$

ou de manière équivalente, de sorte que

$$\sum_{i=1}^{10} i x_i \equiv 0 \ (\text{mod } 11).$$

Répondez à ces questions sur les ISBN-10:

(a) Les neuf premiers chiffres de l'ISBN-10 de la sixième édition de ce livre sont 007288008.
le chiffre de contrôle?

(b) 084930149X est-il un ISBN-10 valide?

Solution: (a) Le chiffre de contrôle est déterminé par la congruence $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$. Insertion les chiffres 007288008 donnent $x_{10} \equiv 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 +$ $9 \cdot 8 \pmod{11}$. Cela signifie que $x_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$, donc $x_{10} \equiv 189 \equiv 2 \pmod{11}$. Par conséquent, $x_{10} = 2$.

(b) Pour voir si 084930149X est un ISBN-10 valide, nous voyons si $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$. nous voir que $1 \cdot 0 + 2 \cdot 8 + 3 \cdot 4 + 4 \cdot 9 + 5 \cdot 3 + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot 4 + 9 \cdot 9 + 10 \cdot 10 = 0 + 16 +$ $12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$Par conséquent, 084930149X n'est pas un ISBN-10 valide. ▲

Plusieurs types d'erreurs surviennent souvent dans les numéros d'identification.Une **seule erreur** , une erreur en une chiffre d'un numéro d'identification, est peut-être le type d'erreur le plus courant.Une autre commune type d'erreur est une **erreur de transposition** , qui se produit lorsque deux chiffres sont accidentellement inter-modifié. Pour chaque type de numéro d'identification, y compris un chiffre de contrôle, nous aimerions être capable de détecter ces types courants d'erreurs, ainsi que d'autres types d'erreurs.Nous enquêterons si le chiffre de contrôle des ISBN peut détecter des erreurs uniques et des erreurs de transpositionQu'il s'agisse les chiffres de contrôle pour les CUP peuvent détecter ces types d'erreurs sont laissés comme exercices 26 et 27.

Les éditeurs le font parfois pas calculer les ISBN correctement pour leurs livres, comme cela a été fait pour un plus tôt édition de ce texte.

Supposons que $x_1 x_2 \ldots x_{10}$ est un ISBN valide (de sorte que $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$). Nous montrerons que nous pouvons détecter une seule erreur et une transposition de deux chiffres (où nous incluons la possibilité que l'un des deux chiffres est le chiffre de contrôle X, représentant 10).Supposons que cet ISBN ait été imprimé avec une seule erreur comme $y_1 y_2 \ldots y_{10}$. S'il y a une seule erreur, alors, pour un entier j , $y_i = x_i$ pour $i = j$ et $y_j = x_j + a$ où $-10 \le a \le 10$ et $a = 0$. Notez que $a = y_j - x_j$ est l'erreur à la j ème place. Il s'ensuit alors que

$$\sum_{i=1}^{\text{ix}} iy_i = \left(\sum_{i=1}^{10} ix_i\right) + ja \equiv ja \equiv 0 \pmod{11}.$$

Ces deux dernières congruences tiennent parce que $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$ et $11 \mid ja$, parce que $11 \mid j$ et $11 \mid a$. Nous concluons que $y_1 y_2 \ldots y_{10}$ n'est pas un ISBN valide. Nous avons donc détecté le single Erreur.

Supposons maintenant que deux chiffres inégaux ont été transposés.Il s'ensuit qu'il existe des des entiers j et k tels que $y_j = x_k$ et $y_k = x_j$, et $y_i = x_i$ pour $i = j$ et $i = k$. Par conséquent,

$$\sum_{i=1}^{\text{ix}} iy_i = \left(\sum_{i=1}^{10} ix_i\right) + (jx_k - jx_j) + (kx_j - kx_k) \equiv (j-k)(x_k - x_j) \equiv 0 \pmod{11},$$

car $\sum_{i=1}^{10} x_i \equiv 0 \pmod{10}$ et $11 \mid (j-k)$ et $11 \mid (x_k - x_j)$. On voit que $y_1 y_2 \ldots y_{10}$ n'est pas un ISBN valide. Ainsi, nous pouvons détecter l'échange de deux chiffres inégaux.

Des exercices

1. Quels emplacements de mémoire sont attribués par le hachage fonction $h(k) = k$ **mod** 97 aux registres d'assurance clients de l'entreprise avec ces numéros de sécurité sociale?

a) 034567981 **b)** 183211232

c) 220195744 **d)** 987255335

2. Quels emplacements de mémoire sont attribués par le hachage fonction $h(k) = k$ **mod** 101 aux registres d'assurance clients de l'entreprise avec ces numéros de sécurité sociale?

a) 104578690 **b)** 432222187

c) 372201919 **d)** 501338753

3. Un parking dispose de 31 places visiteurs, numérotées de 0 à 30. Les visiteurs se voient attribuer des espaces de stationnement à l'aide du hachage fonction $h(k) = k$ **mod** 31, où k est le nombre formé des trois premiers chiffres de la plaque d'immatriculation d'un visiteur.

a) Quels espaces sont attribués par la fonction de hachage à les voitures qui ont ces trois premiers chiffres sur leur permis

7. Quelle séquence de nombres pseudo-aléatoires est utilisant le générateur multiplicatif pur $x_{n+1} =$ $3x_n$ **mod** 11 avec graine $x_0 = 2$?

8. Écrivez un algorithme en pseudocode pour générer un de nombres pseudo-aléatoires en utilisant une congruence générateur intégré.

La **méthode du carré moyen** pour générer un pseudo-aléatoire les nombres commencent par un entier à n chiffres. Ce nombre est au carré, des zéros initiaux sont ajoutés pour garantir que le résultat a $2n$ chiffres, et ses n chiffres du milieu sont utilisés pour former le prochain numéro dans la séquence. Ce processus est répété pour générer conditions supplémentaires.

9. Trouvez les huit premiers termes de la séquence de quatre chiffres nombres pseudo-aléatoires générés par le carré du milieu méthode commençant par 2357.

10. Expliquez pourquoi les deux 3792 et 2916 seraient de mauvais choix pour le terme initial d'une séquence de pseudo-chiffres à quatre chiffres plaques: 317, 918, 007, 100, 111, 310?

b) Décrivez une procédure que les visiteurs doivent suivre pour trouver un espace de stationnement gratuit, lorsque l'espace qui leur est attribué est occupé.

Une autre façon de résoudre les collisions dans le hachage consiste à utiliser le *double hachage* . On utilise une fonction de hachage initiale $h(k) = k$ **mod** p où p est premier. Nous utilisons également une deuxième fonction de hachage $g(k) = (k + 1)$ **mod** $(p - 2)$. Lorsqu'une collision se produit, nous utilisons une *séquence de sondage* $h(k, i) = (h(k) + i \cdot g(k))$ **mod** p .

4. Utilisez la procédure de double hachage que nous avons décrite avec $p = 4969$ pour attribuer des emplacements de mémoire aux fichiers employés avec numéro de sécurité sociale $k_1 = 132489971$, $k_2 = 509496993$, $k_3 = 546332190$, $k_4 = 034367980$, $k_5 = 047900151$, $k_6 = 329938157$, $k_7 = 212228844$, $k_8 = 325510778$, $k_9 = 353354519$, $k_{10} = 053708912$.

5. Quelle séquence de nombres pseudo-aléatoires est utilisant le générateur linéaire congruentiel $x_{n+1} = (3x_n + 2)$ **mod** 13 avec graine $x_0 = 1$?

6. Quelle séquence de nombres pseudo-aléatoires est utilisant le générateur linéaire congruentiel $x_{n+1} = (4x_n + 1)$ **mod** 7 avec graine $x_0 = 3$?

nombres dom générés par la méthode du carré central.

Le **générateur de puissance** est une méthode de génération de pseudo-numéros dom. Pour utiliser le générateur de puissance, les paramètres p et d sont spécifiés, où p est un nombre premier, d est un entier positif tel que $p \mid d$, et une graine x_0 est spécifiée. Le nombre pseudo-aléatoire bers $x_1, x_2, \ldots$ sont générés à l'aide de la définition récursive $x_{n+1} = x_n^d$ **mod** p.

11. Trouver la séquence de nombres pseudo-aléatoires générés par le générateur de puissance avec $p = 7$, $d = 3$ et graine $x_0 = 2$.

12. Trouvez la séquence de nombres pseudo-aléatoires générés par le générateur de puissance avec $p = 11$, $d = 2$ et graine $x_0 = 3$.

13. Supposons que vous ayez reçu ces chaînes de bits sur une communication lien cations, où le dernier bit est un bit de contrôle de parité. Dans quelle chaîne êtes-vous sûr qu'il y a une erreur?

a) 00000111111
b) 10101010101
c) 11111100000
d) 10111101111

14. Prouver qu'un bit de contrôle de parité peut détecter une erreur dans une chaîne si et seulement si la chaîne contient un nombre impair d'erreurs.

Épisode 314

15. Les neuf premiers chiffres de l'ISBN-10 de la version européenne sion de la cinquième édition de ce livre est le 0-07-119881. Quel est le chiffre de contrôle de ce livre?

16. L'ISBN-10 de la sixième édition de *Elementary Number La théorie et ses applications* est 0-321-500Q1-8, où Q est un chiffre. Trouvez la valeur de Q .

17. Déterminez si le chiffre de contrôle de l'ISBN-10 pour ce manuel (la septième édition de *Discrete Mathemat- et ses applications*) a été calculé correctement par le éditeur.

Le United States Postal Service (USPS) vend des mandats identifié par un nombre à 11 chiffres $x_1 x_2 \ldots x_{11}$. Les dix premiers chiffres son identifier le mandat; x_{11} est un chiffre de contrôle qui satisfait $x_{11} = x_1 + x_2 + \cdots + x_{10}$ **mod** 9.

18. Trouvez le chiffre de contrôle pour les mandats USPS qui ont numéro d'identification commençant par ces dix chiffres.

a) 7555618873
b) 6966133421
c) 8018927435
d) 3289744134

19. Déterminez si chacun de ces numéros est un USPS valide numéro d'identification du mandat.

a) 74051489623
b) 88382013445
c) 56152240784
d) 66606631178

20. Un chiffre dans chacun de ces numéros d'identification d'un le mandat postal est taché. Pouvez-vous récupérer le chiffre taché, indiqué par un Q , dans chacun de ces chiffres bers?

a) Q 1223139784
b) 6702120 Q 988
c) 27 Q 41007734
d) 213279032 Q 1

21. Un chiffre dans chacun de ces numéros d'identification d'un le mandat postal est taché. Pouvez-vous récupérer le chiffre taché, indiqué par un Q , dans chacun de ces chiffres bers?

a) 493212 Q 0688
b) 850 Q 9103858
c) 2 Q 941007734
d) 66687 Q 03201

22. Déterminez quelles erreurs à un chiffre sont détectées par le Code de mandat-poste USPS.

23. Déterminez les erreurs de transposition détectées par le Code de mandat-poste USPS.

24. Déterminez le chiffre de contrôle pour les CUP qui ont ces 11 premiers chiffres.

a) 73232184434

a) 036000291452
b) 012345678903
c) 782421843014
d) 726412175425

26. Le chiffre de contrôle d'un code UPC détecte-t-il tous les rors? Prouvez votre réponse ou trouvez un contre-exemple.

27. Déterminez les erreurs de transposition dont le chiffre de contrôle un code UPC trouve.

Certains billets d'avion ont un numéro d'identification à 15 chiffres *un* $_1 a_2 \ldots a_{15}$ où *un* $_{15}$ est un chiffre de contrôle qui est égal à *un* $_1 a_2 \ldots a_{14}$ **mod** 7.

28. Trouvez le chiffre de contrôle a_{15} qui suit chacune de ces 14 chiffres d'un numéro d'identification de billet d'avion.

a) 10237424413392
b) 00032781811234
c) 00611232134231
d) 00193222543435

29. Déterminez si chacun de ces nombres à 15 chiffres est un numéro d'identification de billet d'avion valide.

a) 101333341789013
b) 007862342770445
c) 113273438882531
d) 000122347322871

30. Quelles erreurs dans un seul chiffre d'un billet d'avion à 15 chiffres le numéro d'identification peut être détecté?

∗ **31.** La transposition accidentelle de deux digits consécutifs son dans un numéro d'identification de billet d'avion être détecté en utilisant le chiffre de contrôle?

Les périodiques sont identifiés à l'aide d'une **Norme internationale Numéro de série (ISSN)** . Un ISSN se compose de deux blocs de quatre chiffres. Le dernier chiffre du deuxième bloc est un chèque chiffre. Ce chiffre de contrôle est déterminé par la congruence $d_8 \equiv 3$ *jours* $_1 + 4$ *jours* $_2 + 5$ *jours* $_3 + 6$ *jours* $_4 + 7$ *jours* $_5 + 8$ *jours* $_6 + 9$ *jours* $_7$ (mod 11). Quand $d_8 \equiv 10 \pmod{11}$, nous utilisons la lettre X pour représenter d_8 dans le code.

32. Pour chacun de ces sept premiers chiffres d'un ISSN, déterminez mine le chiffre de contrôle (qui peut être la lettre X).

a) 1570-868
b) 1553-734
c) 1089-708
d) 1383-811

33. Chacun de ces codes à huit chiffres est-il un ISSN possible? Cette est, se terminent-ils par un chiffre de contrôle correct?

a) 1059-1027
b) 0002-9890
c) 1530-8669
d) 1007-120X

34. Le chiffre de contrôle d'un ISSN détecte-t-il chaque erreur

b) 63623991346
c) 04587320720
d) 93764323341

25. Déterminez si chacune des chaînes de 12 chiffres est un code UPC valide.

dans un ISSN? Justifiez votre réponse avec une preuve ou un contre-exemple.

35. Le chiffre de contrôle d'un ISSN détecte-t-il toutes les erreurs deux chiffres consécutifs sont accidentellement échangés? Jus-Justifiez votre réponse avec une preuve ou un contre-exemple.

Cryptographie

introduction

La théorie des nombres joue un rôle clé dans la cryptographie, le sujet de la transformation de l'information afin que il ne peut pas être facilement récupéré sans connaissances particulières.La théorie des nombres est à la base de chiffres classiques, utilisés pour la première fois il y a des milliers d'années, et largement utilisés jusqu'au 20e siècle. Ces chiffres chiffrent les messages en changeant chaque lettre en une lettre différente, ou chaque bloc de lettres à un autre bloc de lettres. Nous allons discuter de quelques chiffrements classiques, y compris shift chiffres, qui remplacent chaque lettre par la lettre un nombre fixe de positions plus tard dans l'alphabet, enrouler autour du début de l'alphabet si nécessaire. Les chiffres classiques que nous allons discuter sont des exemples de chiffrement de clé privée où savoir comment chiffrer permet à quelqu'un de décrypter également les messages. Avec un chiffrement à clé privée, deux parties qui souhaitent communiquer en secret doit partager une clé secrète. Les chiffres classiques dont nous parlerons sont également vulnérables à la cryptanalyse, qui cherche à récupérer des informations cryptées sans accès aux informations secrètes utilisées pour crypter le message. Nous allons montrer comment chiffrer les messages envoyés à l'aide de chiffres de décalage.

La théorie des nombres est également importante dans la cryptographie à clé publique, un type de cryptographie inventé dans les années 1970. En cryptographie à clé publique, savoir chiffrer ne dit pas non plus à quelqu'un comment décrypter. Le système de clé publique le plus utilisé, appelé le cryptosystème RSA, crypte messages utilisant l'exponentiation modulaire, où le module est le produit de deux grands nombres premiers. Savoir chiffrer nécessite que quelqu'un connaisse le module et un exposant.(Cela fait pas que les deux facteurs premiers du module soient connus.) Pour autant que l'on sache, sachant comment décrypter nécessite que quelqu'un sache comment inverser la fonction de cryptage, qui ne peut être fait dans un laps de temps pratique lorsque quelqu'un connaît ces deux grands facteurs premiers.Dans ce chapitre, nous expliquerons comment fonctionne le cryptosystème RSA, y compris comment chiffrer et décrypter les messages.

Le sujet de la cryptographie comprend également le sujet des protocoles cryptographiques, qui sont échanges de messages effectués par deux ou plusieurs parties pour atteindre un objectif de sécurité spécifique.nous discutera de deux protocoles importants dans ce chapitre. On permet à deux personnes de partager un commun clef secrète. L'autre peut être utilisé pour envoyer des messages signés afin qu'un destinataire puisse être sûr que ils ont été envoyés par le prétendu expéditeur.

Cryptographie classique

L'une des premières utilisations connues de la cryptographie a été celle de Jules César.Il a fait des messages secrets en décalant chaque lettre de trois lettres vers l'avant dans l'alphabet (en envoyant les trois dernières lettres du alphabet aux trois premiers). Par exemple, en utilisant ce schéma, la lettre B est envoyée à E et la lettre X est envoyé à A. C'est un exemple de**cryptage** , c'est-à-dire le processus de secret d'un message.

Pour exprimer mathématiquement le processus de cryptage de César, remplacez d'abord chaque lettre par un élément. ment de $\mathbf{Z}_{26}$, c'est-à-dire un entier de 0 à 25 égal à un de moins que sa position dans l'alphabet.Pour par exemple, remplacez A par 0, K par 10 et Z par 25. La méthode de cryptage de César peut être représentée par la fonction f qui affecte à l'entier non négatif p , $p \leq 25$, l'entier $f(p)$ dans l'ensemble $\{0, 1, 2, ..., 25\}$ avec

$$f(p) = (p + 3) \textbf{ mod } 26.$$

Dans la version cryptée du message, la lettre représentée par$p$ est remplacée par la lettre représenté par $(p + 3)$ **mod** 26.

EXEMPLE 1 Quel est le message secret produit à partir du message "MEET YOU IN THE PARK" en utilisant le chiffre de César?

Solution: remplacez d'abord les lettres du message par des chiffres.Cela produit

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10 .

Remplacez maintenant chacun de ces nombres p par $f(p) = (p + 3)$ **mod** 26. Cela donne

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13 .

La traduction de ce retour en lettres produit le message crypté «PHHW BRX LQ WKH SDUN. " ▲

Pour récupérer le message d'origine à partir d'un message secret chiffré par le chiffre César, le fonction f^{-1} , l'inverse de f , est utilisé. Notez que la fonction f^{-1} envoie un entier p de $\mathbf{Z}_{26}$, à $f^{-1}(p) = (p - 3)$ **mod** 26. En d'autres termes, pour trouver le message d'origine, chaque lettre est reculé de trois lettres dans l'alphabet, les trois premières lettres étant envoyées aux trois dernières lettres de l'alphabet. Processus de détermination du message d'origine à partir du message chiffré est appelé **décryptage** .

Il existe différentes façons de généraliser le chiffre César. Par exemple, au lieu de déplacer la l'équivalent numérique de chaque lettre par 3, nous pouvons déplacer l'équivalent numérique de chaque lettre de k , de sorte que

$f(p) = (p + k)$ **mod** 26 .

Un tel chiffre est appelé *chiffre à décalage* . Notez que le déchiffrement peut être effectué en utilisant

$f^{-1}(p) = (p - k)$ **mod** 26 .

Ici, l'entier k est appelé une **clé** . Nous illustrons l'utilisation d'un chiffre de décalage dans les exemples 2 et 3.

EXEMPLE 2 Crypter le message en clair «STOP GLOBAL WARMING» en utilisant le chiffre shift avec shift $k = 11$.

Solution: pour crypter le message «ARRÊTER LE RÉCHAUFFEMENT MONDIAL», nous traduisons d'abord chaque lettre à l'élément correspondant de $\mathbf{Z}_{26}$. Cela produit la chaîne

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6 .

Nous appliquons maintenant le décalage $f(p) = (p + 11)$ **mod** 26 à chaque nombre de cette chaîne. On obtient

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17 .

En traduisant cette dernière chaîne en lettres, nous obtenons le texte chiffré «DEZA RWZMLW HLCX-TYR. " ▲

EXEMPLE 3 Décrypter le message de texte chiffré «LEWLYPLUJL PZ H NYLHA ALHJOLY» qui était crypté avec le chiffre de décalage avec décalage $k = 7$.

Solution: Pour déchiffrer le texte chiffré "LEWLYPLUJL PZ H NYLHA ALHJOLY", nous devons d'abord traduire les lettres en éléments de $\mathbf{Z}_{26}$. On obtient

11 4 22 11 24 15 11 20 9 11 15 25 sept 13 24 11 7 0 0 11 7 9 14 11 24 .

Ensuite, nous décalons chacun de ces nombres de $-k = -7$ modulo 26 pour obtenir

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17 .

Enfin, nous traduisons ces chiffres en lettres pour obtenir le texte en clair.On obtient "L'EXPÉRIENCE EST UN GRAND ENSEIGNANT." ▲

Nous pouvons généraliser davantage les chiffres de décalage pour améliorer légèrement la sécurité en utilisant une fonction de la forme

$$f(p) = (ap + b) \textbf{ mod } 26,$$

où a et b sont des entiers, choisis pour que f soit une bijection. (La fonction $f(p) = (ap + b)$ le **mod** 26 est une bijection si et seulement si gcd $(a, 26) = 1$.) Une telle cartographie est appelée *affine transformation* , et le chiffre résultant est appelé un *chiffre affine* .

EXEMPLE 4 Quelle lettre remplace la lettre K lorsque la fonction $f(p) = (7p + 3)$ **mod** 26 est utilisée pour cryption?

Solution: notez d'abord que 10 représente K. Ensuite, en utilisant la fonction de chiffrement spécifiée, il suit que $f(10) = (7 \cdot 10 + 3)$ **mod** 26 = 21. Parce que 21 représente V, K est remplacé par V dans le message crypté. ▲

Nous allons maintenant montrer comment déchiffrer les messages chiffrés à l'aide d'un chiffrement affine.Supposer que $c = (ap + b)$ **mod** 26 avec gcd $(a, 26) = 1$. Pour décrypter, nous devons montrer comment exprimer p dans termes de c . Pour ce faire, nous appliquons la congruence de chiffrement $c \equiv ap + b \pmod{26}$, et la résolvons pour p . Pour ce faire, on soustrait d'abord b des deux côtés, pour obtenir $c - b \equiv ap \pmod{26}$. Car pgcd $(a, 26) = 1$, on sait qu'il y a l'inverse $\bar{a}$ d' *un* modulo 26. Multipliant les deux côtés de la dernière équation de $\bar{a}$ nous donne $\bar{a}(c - b) \equiv \bar{a}ap \pmod{26}$. Parce que $\bar{a}a \equiv 1 \pmod{26}$, cela indique nous que $p \equiv \bar{a}(c - b) \pmod{26}$. Cela détermine p car p appartient à $\mathbf{Z}_{26}$.

CRYPTANALYSE Processus de récupération de texte en clair à partir d'un texte chiffré sans connaissance La méthode de cryptage et la clé sont connues sous le nom de **crypto - analyse** ou de **rupture des codes** . Dans en général, la cryptanalyse est un processus difficile, surtout lorsque la méthode de cryptage est inconnue. Nous ne discuterons pas de la cryptanalyse en général, mais nous expliquerons comment briser les messages ont été chiffrés à l'aide d'un chiffre de décalage.

Si nous savons qu'un message chiffré a été produit en chiffrant un message à l'aide d'un décalage chiffrement, nous pouvons essayer de récupérer le message en déplaçant tous les caractères du texte chiffré par chacun des 26 décalages possibles (y compris un décalage de zéro caractère).L'un d'eux est garanti le texte en clair. Cependant, nous pouvons utiliser une approche plus intelligente, sur laquelle nous pouvons chiffrer le texte chiffré résultant d'autres chiffres. L'outil principal pour chiffrer le texte chiffré chiffré à l'aide d'un chiffre de décalage est le compte de la fréquence des lettres dans le texte chiffréLes neuf les lettres les plus courantes dans le texte anglais et leurs fréquences relatives approximatives sont E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6% et R 6%.Pour chiffrer le texte chiffré que nous savons être produit à l'aide d'un chiffre de décalage, nous trouvons d'abord les fréquences relatives des lettres dans le texte chiffré. Nous listons les lettres les plus courantes dans le texte chiffré par ordre de fréquence;nous supposons que le la lettre la plus courante dans le texte chiffré est produite en chiffrant E. Ensuite, nous déterminons la valeur du décalage sous cette hypothèse, disons k . Si le message produit en déplaçant le texte chiffré by $-k$ est logique, nous supposons que notre hypothèse est correcte et que nous avons la bonne valeur de k . Si cela n'a pas de sens, nous considérons ensuite l'hypothèse selon laquelle la plus courante la lettre du texte chiffré est produite en chiffrant T, la deuxième lettre la plus courante en anglais; nous trouvons k sous cette hypothèse, décalons les lettres du message de $-k$, et voyons si le le message qui en résulte est logique. Si ce n'est pas le cas, nous continuons le processus de les lettres du plus commun au moins commun.

Les mathématiciens font le meilleurs disjoncteurs de code.Leur travailler pendant la Seconde Guerre mondiale changé le cours de la guerre.

EXEMPLE 5 Supposons que nous ayons intercepté le message chiffré ZNK KGXRE HOXJ MKZY ZNK CUXS que nous savons a été produit par un chiffre de décalage. Quel était le message en texte brut d'origine?

Solution: car nous savons que le message chiffré intercepté a été chiffré à l'aide d'un décalage du chiffre, nous commençons par calculer la fréquence des lettres dans le texte chiffré. Nous constatons que la lettre la plus courante dans le texte chiffré est K. Donc, nous émettons l'hypothèse que le chiffre de décalage envoyé la lettre en clair E à la lettre de chiffrement K. Si cette hypothèse est correcte, nous savons que $10 = 4 + k$ **mod** 26, donc $k = 6$. Ensuite, nous décalons les lettres du message de −6, obtenant LE MONDE APPARTIENT À CEUX QUI SE LÈVENT TÔT. Parce que ce message est logique, nous supposons que l'hypothèse que $k = 6$ est correcte. ▲

BLOC CIPHERS **Chiffres décalés** et chiffrements **affins** procéder en remplaçant chaque lettre du alphabet par une autre lettre de l'alphabet. Pour cette raison, ces chiffres sont appelés **caractère** ou des **chiffres monoalphabétiques** . Les méthodes de chiffrement de ce type sont vulnérables aux attaques basées sur sur l'analyse de la fréquence des lettres dans le texte chiffré, comme nous venons de l'illustrer. On peut le faire plus difficile d'attaquer avec succès le texte chiffré en remplaçant des blocs de lettres par d'autres blocs de lettres au lieu de remplacer des caractères individuels par des caractères individuels; ces chiffres sont appelés **chiffres de bloc** .

Nous allons maintenant introduire un type simple de chiffrement par blocs, appelé **chiffrement de transposition** . Comme une clé, nous utilisons une permutation σ de l'ensemble $\{1, 2, ..., m\}$ pour un entier positif m, c'est-à-dire un fonction un à un de $\{1, 2, ..., m\}$ à lui-même. Pour crypter un message, nous avons d'abord divisé ses lettres en blocs de taille m. (Si le nombre de lettres dans le message n'est pas divisible par m on ajoute quelques lettres aléatoires à la fin pour remplir le bloc final.) On crypte le bloc $p_1 p_2 ... p_m$ comme $c_1 c_2 ... c_m = p_{\sigma(1)} p_{\sigma(2)} ..., p_{\sigma(m)}$. Pour décrypter un bloc de texte chiffré $c_1 c_2 ... c_m$, on transpose ses lettres en utilisant la permutation σ^{-1}, l'inverse de σ. L'exemple 6 illustre le chiffrement et décryptage pour un chiffrement de transposition.

EXEMPLE 6 En utilisant le chiffrement de transposition basé sur la permutation σ de l'ensemble $\{1, 2, 3, 4\}$ avec $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$ et $\sigma(4) = 2$,

(a) Crypter le message en clair PIRATE ATTACK.

(b) Déchiffrer le message de chiffrement SWUE TRAE OEHS, qui a été chiffré à l'aide de ce chiffrement.

Solution: (a) Nous avons d'abord divisé les lettres du texte en clair en blocs de quatre lettres. Nous obtenons PIRA TEAT TACK. Pour crypter chaque bloc, nous envoyons la première lettre à la troisième position, la deuxième lettre à la première position, la troisième lettre à la quatrième position et la quatrième lettre à la deuxième position. Nous obtenons IAPR ETTA AKTC.

(b) On note que σ^{-1}, l'inverse de σ, envoie 1 à 2, envoie 2 à 4, envoie 3 à 1 et envoie 4 à 3. L'application de $\sigma^{-1}(m)$ à chaque bloc nous donne le texte en clair: USEW ATER HOSE. (Regroupement ensemble ces lettres pour former des mots communs, nous supposons que le texte en clair est UTILISER L'EAU TUYAU.) ▲

CRYPTOSYSTEMES Nous avons défini deux familles de chiffres: les chiffres à décalage et les chiffres affins. Nous introduisons maintenant la notion de cryptosystème, qui fournit une structure générale pour définir nouvelles familles de chiffres.

DÉFINITION 1 Un *cryptosystème* est un tuple (P, C, K, E, D), où P est l'ensemble des chaînes de texte en clair, C est l'ensemble des chaînes de texte chiffré, K est l'*espace de clés* (l'ensemble de toutes les clés possibles), E est l'ensemble de fonctions de cryptage, et D est l'ensemble des fonctions de décryptage. On note E_k le cryptage fonction en E correspondant à la clé k et D_k la fonction de décryptage en D qui décrypte texte chiffré qui a été chiffré à l'aide de E_k, c'est-à-dire $D_k(E_k(p)) = p$, pour toutes les chaînes de texte en clair p.

Nous illustrons maintenant l'utilisation de la définition d'un cryptosystème.

EXEMPLE 7 Décrire la famille des chiffres de décalage comme un cryptosytème.

Solution: pour crypter une chaîne de lettres anglaises avec un chiffre de décalage, nous traduisons d'abord chaque lettre à un entier compris entre 0 et 25, c'est-à-dire à un élément de $\mathbf{Z}_{26}$. On décale ensuite chacun de ces entiers par un entier fixe modulo 26, et enfin, nous traduisons les entiers en lettres. Pour appliquer le définition d'un cryptosystème pour déplacer les chiffres, nous supposons que nos messages sont déjà des entiers, c'est-à-dire des éléments de $\mathbf{Z}_{26}$. Autrement dit, nous supposons que la traduction entre les lettres et les entiers est en dehors du cryptosystème. Par conséquent, à la fois l'ensemble des chaînes de texte en clair P et l'ensemble des les chaînes de texte chiffré C sont l'ensemble des chaînes d'éléments de $\mathbf{Z}_{26}$. L'ensemble des clés K est l'ensemble des possibles décale, donc $K = \mathbf{Z}_{26}$. L'ensemble E est constitué de fonctions de la forme $E_k(p) = (p + k)$ **mod** 26, et l'ensemble D des fonctions de déchiffrement est le même que l'ensemble des fonctions de chiffrement où $D_k(p) = (p - k)$ **mod** 26. ▲

Le concept de cryptosystème est utile dans la discussion de familles supplémentaires de chiffres et est largement utilisé en cryptographie.

Cryptographie à clé publique

Tous les chiffres classiques, y compris les chiffres de décalage et les chiffres affins, sont des exemples de **clé privée cryptosystèmes** . Dans un cryptosystème à clé privée, une fois que vous connaissez une clé de cryptage, vous pouvez trouver rapidement la clé de déchiffrement. Donc, savoir chiffrer les messages à l'aide d'une clé particulière vous permet de déchiffrer les messages chiffrés à l'aide de cette clé. Par exemple, lorsqu'un quart de travail le chiffrement est utilisé avec la clé de chiffrement k , l'entier en texte brut p est envoyé à

$$c = (p + k) \textbf{ mod } 26 .$$

Le déchiffrement est effectué en décalant de $-k$; C'est,

$$p = (c - k) \textbf{ mod } 26 .$$

Donc, savoir comment chiffrer avec un chiffre de décalage vous indique également comment déchiffrer.

Lorsqu'un cryptosystème à clé privée est utilisé, deux parties qui souhaitent communiquer en secret doit partager une clé secrète. Parce que quiconque connaît cette clé peut à la fois crypter et décrypter messages, deux personnes qui souhaitent communiquer en toute sécurité doivent échanger cette clé en toute sécurité. (Nous présenterons une méthode pour le faire plus tard dans cette section.) Le chiffre de décalage et le chiffre affine Les cryptosystèmes sont des cryptosystèmes à clé privée. Ils sont assez simples et extrêmement vulnérables à la cryptanalyse. Cependant, la même chose n'est pas vraie de nombreux cryptosystèmes à clé privée modernes. Dans en particulier, la norme actuelle du gouvernement américain pour la cryptographie à clé privée, Advanced Encryption Standard (AES), est extrêmement complexe et est considéré comme très résistant aux cryptanalyse. (Voir [St06] pour plus de détails sur AES et d'autres cryptosystèmes à clé privée modernes.) AES est largement utilisé dans les communications gouvernementales et commerciales. Cependant, il partage toujours la propriété de partage des clés de communication sécurisées. De plus, pour plus de sécurité, un une nouvelle clé est utilisée pour chaque session de communication entre deux parties, ce qui nécessite une méthode pour générer des clés et les partager en toute sécurité.

Pour éviter que les clés ne soient partagées par toutes les parties qui souhaitent communiquer en toute sécurité, dans les années 1970, les cryptologues ont introduit le concept de **cryptosystèmes à clé publique** . Quand de tels cryptosystèmes sont utilisés, savoir comment envoyer un message crypté n'aide pas à décrypter messages. Dans un tel système, tout le monde peut avoir une clé de chiffrement connue du public. Seulement le les clés de déchiffrement sont gardées secrètes et seul le destinataire prévu d'un message peut le déchiffrer, car, dans la mesure où il est actuellement connu, la connaissance de la clé de chiffrement ne permet pas à quelqu'un récupérer le message en clair sans une quantité extraordinaire de travail (comme des milliards de ans d'ordinateur).

Le cryptosystème RSA

Le MIT est également connu sous le nom de le 'Tute.

En 1976, trois chercheurs du Massachusetts Institute of Technology - Ronald Rivest, Adi Shamir et Leonard Adleman — ont présenté au monde un cryptosystème à clé publique, connu sous le nom de **Système RSA** , d'après les initiales de ses inventeurs. Comme cela arrive souvent avec les découvertes cryptographiques, le système RSA avait été découvert plusieurs années plus tôt dans la recherche secrète du gouvernement dans le Royaume-Uni. Clifford Cocks, travaillant en secret au gouvernement du Royaume-Uni Communications Headquarters (GCHQ), avait découvert ce cryptosystème en 1973. Cependant, son invention était inconnue du monde extérieur jusqu'à la fin des années 1990, quand il a été autorisé à partager des documents classifiés du GCHQ du début des années 1970. (Un excellent compte rendu de cela plus tôt découverte, ainsi que les travaux de Rivest, Shamir et Adleman, peuvent être trouvés dans [Si99].)

Malheureusement, personne appelle cela les coqs cryptosystème.

Dans le cryptosystème RSA, chaque individu possède une clé de cryptage (n, e) où $n = pq$, le module est le produit de deux grands nombres premiers p et q , disons avec 200 chiffres chacun, et un exposant e qui est relativement premier à $(p - 1)(q - 1)$. Pour produire une clé utilisable, deux grands nombres premiers doivent être a trouvé. Cela peut être fait rapidement sur un ordinateur en utilisant des tests de primalité probabilistes, plus haut dans cette section. Cependant, le produit de ces nombres premiers $n = pq$, avec environ 400

pour autant que l'on sache actuellement, les chiffres ne peuvent pas être pris en compte dans un délai raisonnableComme nous
verra, c'est une raison importante pour laquelle le déchiffrement ne peut pas, pour autant que l'on sache actuellement,
fait rapidement sans clé de déchiffrement séparée.

Cryptage RSA

Pour crypter les messages à l'aide d'une clé particulière (n, e), nous traduisons d'abord un message en clair M en séquences d'entiers. Pour ce faire, nous traduisons d'abord chaque lettre en clair en deux chiffres nombre, en utilisant la même traduction que nous avons utilisée pour les chiffres de décalage, avec une différence clé. Autrement dit, nous incluons un zéro initial pour les lettres A à J, de sorte que A est traduit en 00, B en 01, ... et J en 09. Ensuite, nous enchaînons ces nombres à deux chiffres en chaînes de chiffres. Ensuite, nous divisons cette chaîne en blocs de taille égale de $2N$ chiffres, où $2N$ est le plus grand pair nombre tel que le nombre 2525 ... 25 avec $2N$ chiffres ne dépasse pas n. (Quand c'est nécessaire, nous remplissons le message en clair avec des X factices pour que le dernier bloc ait la même taille que tous les autres blocs.)

Après ces étapes, nous avons traduit le message en clair M en une séquence d'entiers $m_1, m_2, \ldots, m_k$ pour un entier k. Le chiffrement se poursuit en transformant chaque bloc m_i en un bloc de texte chiffré c_i. Cela se fait en utilisant la fonction

$$C = M^e \ \mathbf{mod}\ n.$$

(Pour effectuer le chiffrement, nous utilisons un algorithme d'exponentiation modulaire rapide, tel que Algorithme 5 de la section 4.2.) Nous laissons le message crypté sous forme de blocs de chiffres et envoyons ceux-ci au destinataire prévu. Parce que le cryptosystème RSA crypte des blocs de caractères en blocs de caractères, c'est un chiffrement par blocs.

CLIFFORD COCKS (NÉ EN 1950) Clifford Cocks, né à Cheshire, en Angleterre, était un talentueux mathématicien étudiant. En 1968, il a remporté une médaille d'argent à l'Olympiade mathématique internationale. Les bites ont assisté à King's Collège, Cambridge, étudiant les mathématiques. Il a également passé un peu de temps à l'Université d'Oxford à travailler théorie. En 1973, il a décidé de ne pas terminer ses études supérieures, mais de prendre un emploi de mathématique au ment des communications (GCHQ) du renseignement britannique. Deux mois après avoir rejoint le GCHQ, Cocks découvert la cryptographie à clé publique grâce à un rapport interne du GCHQ rédigé par James Ellis. Cocks a utilisé son connaissances en théorie des nombres pour inventer ce qui est maintenant appelé le cryptosystème RSA. Il a rapidement réalisé qu'un public le cryptosystème clé pourrait être basé sur la difficulté d'inverser le processus de multiplication de deux grands nombres premiers. Dans 1997, il a été autorisé à révéler des documents internes déclassifiés du GCHQ décrivant sa découverte. Cocks c'est aussi connu pour son invention d'un schéma de chiffrement basé sur l'identité sécurisée, qui utilise des informations sur l'identité d'un utilisateur comme clé publique. En 2001, Cocks est devenu le mathématicien en chef du GCHQ. Il a également créé l'Institut Heilbronn pour la recherche mathématique, un partenariat entre le GCHQ et l'Université de Bristol.

L'exemple 8 illustre comment le chiffrement RSA est effectué.Pour des raisons pratiques, nous utilisons de petites prime p et q dans cet exemple, plutôt que prime à 200 chiffres ou plus.Bien que le chiffre décrit dans cet exemple n'est pas sécurisé, il illustre bien les techniques utilisées dans le chiffrement RSA.

EXEMPLE 8 Crypter le message STOP à l'aide du cryptosystème RSA avec clé $(2537, 13)$. Notez que $2537 = 43 \cdot 59$, $p = 43$ et $q = 59$ sont des nombres premiers, et

$$\text{pgcd}(e, (p-1)(q-1)) = \text{pgcd}(13, 42 \cdot 58) = 1.$$

Solution: Pour chiffrer, nous traduisons d'abord les lettres en STOP en leurs équivalents numériques.nous puis regroupez ces nombres en blocs de quatre chiffres (car $2525 < 2537 < 252525$), pour obtenir

1819 1415 .

Nous chiffrons chaque bloc en utilisant la cartographie

$$C = M^{13} \ \mathbf{mod}\ 2537.$$

Les calculs utilisant la multiplication modulaire rapide montrent que 1819^{13} **mod** $2537 = 2081$ et 1415^{13} **mod** $2537 = 2182$. Le message crypté est 2081 2182. ▲

Déchiffrement RSA

Le message en clair peut être récupéré rapidement à partir d'un message chiffré lorsque le déchiffrement la clé de *dation*, inverse de e modulo $(p-1)(q-1)$, est connue. [Un tel inverse existe parce que gcd $(e, (p-1)(q-1)) = 1$.] Pour voir cela, notez que si $de \equiv 1 \pmod{(p-1)(q-1)}$, il y a un entier k tel que $de = 1 + k(p-1)(q-1)$. Il s'ensuit que

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod n.$$

RONALD RIVEST (NÉ EN 1948) Ronald Rivest a obtenu un BA de Yale en 1969 et son doctorat. dans l'ordinateur science de Stanford en 1974. Rivest est professeur d'informatique au MIT et a été cofondateur de RSA Data Security, qui détenait le brevet sur le cryptosystème RSA qu'il a inventé avec Adi Shamir et Leonard Adleman. Outre la cryptographie, Rivest a travaillé dans des domaines tels que l'apprentissage automatique, la conception VLSI et algorithmes informatiques. Il est co-auteur d'un texte populaire sur les algorithmes ([CoLeRiSt09]).

ADI SHAMIR (NÉ EN 1952) Adi Shamir est né à Tel Aviv, en Israël. Son diplôme de premier cycle est de Université de Tel Aviv (1972) et son doctorat. est du Weizmann Institute of Science (1977). Shamir était un assistant de recherche à l'Université de Warwick et professeur adjoint au MIT. Il est actuellement professeur au département de mathématiques appliquées de l'Institut Weizmann et dirige un groupe étudiant l'informatique Sécurité. Les contributions de Shamir à la cryptographie, outre le cryptosystème RSA, comprennent le craquage du sac à dos cryptosystèmes, la cryptanalyse du Data Encryption Standard (DES) et la conception de nombreux systèmes cryptographiques protocoles.

LEONARD ADLEMAN (NÉ EN 1945) Leonard Adleman est né à San Francisco, en Californie. Il a reçu un BS en mathématiques (1968) et son doctorat. en informatique (1976) de l'Université de Californie, Berkeley. Adleman a été membre de la faculté de mathématiques du MIT de 1976 à 1980, où il était un co-inventeur du cryptosystème RSA, et en 1980, il a pris une position dans le département d'informatique à l'Université de Californie du Sud (USC). Il a été nommé à un poste de président de l'USC en 1985. Adleman a travaillé sur la sécurité informatique, la complexité informatique, l'immunologie et la biologie moléculaire. Il a inventé le terme «virus informatique». Les travaux récents d'Adleman sur le calcul de l'ADN ont suscité un grand intérêt. Il était un conseiller technique pour le film *Sneakers* , dans lequel la sécurité informatique a joué un rôle important.

Par le petit théorème de Fermat [en supposant que gcd(M, p) = gcd (M, q) = 1, qui tient sauf dans cas rares, que nous couvrons dans l'exercice 28], il s'ensuit que $M^{p-1} \equiv 1 \pmod p$ et $M^{q-1} \equiv 1 \pmod q$. Par conséquent,

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod p$$

et

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod q.$$

Parce que gcd $(p, q) = 1$, il s'ensuit par le théorème du reste chinois que

$$C^d \equiv M \pmod{pq}.$$

L'exemple 9 illustre comment déchiffrer les messages envoyés à l'aide du cryptosystème RSA.

EXEMPLE 9 Nous recevons le message crypté 0981 0461. Quel est le message décrypté s'il a été crypté en utilisant le chiffrement RSA de l'exemple 8?

Solution: le message a été chiffré à l'aide du cryptosystème RSA avec $n = 43 \cdot 59$ et expo nent 13. Comme le montre l'exercice 2 de la section 4.4, $d = 937$ est l'inverse de 13 modulo $42 \cdot 58 = 2436$. Nous utilisons 937 comme exposant de décryptage. Par conséquent, pour déchiffrer un bloc C, nous calculons

$$M = C^{937} \mathbf{mod}\ 2537.$$

Pour déchiffrer le message, nous utilisons l'algorithme d'exponentiation modulaire rapide pour calculer 0981^{937} **mod** 2537 = 0704 et 0461^{937} **mod** 2537 = 1115. Par conséquent, la version numérique du message d'origine est 0704 1115. En traduisant ce message en lettres anglaises, nous voyons que le le message est AIDE. ▲

RSA en tant que système de clé publique

Pourquoi le cryptosystème RSA convient-il à la cryptographie à clé publique? Premièrement, il est possible de rapidement construire une clé publique en trouvant deux grands nombres premiers p et q, chacun avec plus de 200 chiffres, et pour trouver un entier e relativement premier à $(p - 1)(q - 1)$. Quand on connaît la factorisation de le module n, c'est-à-dire que lorsque nous connaissons p et q, nous pouvons trouver rapidement un inverse d de e modulo $(p - 1)(q - 1)$. [Cela se fait en utilisant l'algorithme euclidien pour trouver les coefficients de Bézout s et t pour d et $(p - 1)(q - 1)$, ce qui montre que l'inverse de d modulo $(p - 1)(q - 1)$ est s **mod** $(p - 1)(q - 1)$.] La connaissance de d nous permet de décrypter les messages envoyés à l'aide de notre clé. Cependant, non est connue pour décrypter les messages qui ne sont pas basés sur la recherche d'une factorisation de n, ou ne conduit pas non plus à la factorisation de n.

La factorisation est considérée comme un problème difficile, par opposition à la recherche de grands nombres premiers p

et q , ce qui peut être fait rapidement. Les méthodes de factorisation les plus efficaces connues (à partir de 2010) nécessitent des milliards d'années pour factoriser des entiers à 400 chiffres. Par conséquent, lorsque p et q sont à 200 chiffres premiers, on pense que les messages chiffrés en utilisant $n = pq$ comme module ne peuvent pas être trouvés dans un temps raisonnable à moins que les nombres premiers p et q soient connus.

Bien qu'aucun algorithme à temps polynomial ne soit connu pour la factorisation de grands entiers, des recherches sont en cours pour trouver de nouvelles façons de factoriser efficacement les entiers. Des nombres entiers pensés, comme récemment comme il y a plusieurs années, être beaucoup trop important pour être pris en compte dans un délai raisonnable peut maintenant être pris en compte régulièrement. Entiers de plus de 150 chiffres, ainsi que certains de plus de 200 chiffres, ont été factorisés grâce aux efforts de l'équipe. Lorsque de nouvelles techniques de factorisation sont trouvées,

il sera nécessaire d'utiliser des nombres premiers plus grands pour garantir la confidentialité des messages. Malheureusement, les messages qui étaient considérés comme sûrs auparavant peuvent être sauvegardés puis décryptés par des destinataires lorsqu'il devient possible de prendre en compte le $n = pq$ dans la clé utilisée pour le chiffrement RSA.

La méthode RSA est désormais largement utilisée. Cependant, les cryptosystèmes les plus couramment utilisés sont des cryptosystèmes à clé privée. L'utilisation de la cryptographie à clé publique, via le système RSA, est croissance. Néanmoins, il existe des applications qui utilisent à la fois des systèmes à clé privée et des systèmes à clé publique. Par exemple, un cryptosystème à clé publique, tel que RSA, peut être utilisé pour distribuer des clés privées à des paires de personnes qui souhaitent communiquer. Ces personnes utilisent ensuite une clé privée système de cryptage et de décryptage des messages.

Protocoles cryptographiques

Jusqu'à présent, nous avons montré comment la cryptographie peut être utilisée pour sécuriser les messages. cependant, il existe de nombreuses autres applications importantes de la cryptographie. Parmi ces applications figurent **protocoles cryptographiques** , qui sont des échanges de messages effectués par deux ou plusieurs parties pour atteindre un objectif de sécurité particulier. En particulier, nous montrerons comment la cryptographie peut être utilisée pour permettre à deux personnes d'échanger une clé secrète sur un canal de communication non sécurisé. Nous allons montrer également comment la cryptographie peut être utilisée pour envoyer des messages secrets signés afin que le destinataire peut être sûr que le message provient de l'expéditeur présumé. Nous renvoyons le lecteur à [St05] pour des discussions approfondies sur une variété de protocoles cryptographiques.

ÉCHANGE DE CLÉS Nous discutons maintenant d'un protocole que deux parties peuvent utiliser pour échanger un secret sur un canal de communication non sécurisé sans avoir partagé aucune information dans le passé. La génération d'une clé que deux parties peuvent partager est importante pour de nombreuses applications de cryptage. tographie. Par exemple, pour que deux personnes s'envoient des messages sécurisés à l'aide d'un cryptosystème clé dont ils ont besoin pour partager une clé commune. Le protocole que nous allons décrire est connu sous le nom de le **protocole d'accord clé Diffie-Hellman** , après Whitfield Diffie et Martin Hellman, qui l'a décrit en 1976. Cependant, ce protocole a été inventé en 1974 par Malcolm Williamson dans travail secret au GCHQ britannique. Ce n'est qu'en 1997 que sa découverte a été rendue publique.

Supposons qu'Alice et Bob souhaitent partager une clé commune. Le protocole suit ces étapes, où les calculs se font en $\mathbf{Z}_p$.

(1) Alice et Bob conviennent d'utiliser un p premier et une racine primitive a de p .

(2) Alice choisit un entier secret k_1 et envoie un^{k_1} **mod** p à Bob.

(3) Bob choisit un entier secret k_2 et envoie un^{k_2} **mod** p à Alice.

(4) Alice calcule $(a^{k_2})^{k_1}$ **mod** p .

(5) Bob calcule $(a^{k_1})^{k_2}$ **mod** p .

À la fin de ce protocole, Alice et Bob ont calculé leur clé partagée, à savoir

$$(a^{k_2})^{k_1} \bmod p = (a^{k_1})^{k_2} \bmod p.$$

Pour analyser la sécurité de ce protocole, notez que les messages envoyés aux étapes (1), (2) et (3) ne sont pas supposés être envoyés en toute sécurité. On peut même supposer que ces communications étaient en clair et que leur contenu est une information publique. Donc, p , a , a^{k_1} **mod** p , et a^{k_2} **mod** p sont supposés être des informations publiques. Le protocole garantit que k_1 , k_2 et la clé commune $(a^{k_2})^{k_1}$ **mod** $p = (a^{k_1})^{k_2}$ **mod** p sont gardés secrets. Pour trouver les informations secrètes de ce pub-

Les informations licites exigent qu'un adversaire résout des cas du problème du logarithme discret,

parce que l'adversaire devrait trouver k_1 et k_2 à partir d' un^{k_1} **mod** p et d' un^{k_2} **mod** p , respec-
activement. En outre, aucune autre méthode n'est connue pour trouver la clé partagée en utilisant uniquement le public information. Nous avons remarqué que cela est considéré comme impossible à calculer lorsque p et a sont suffisamment grands. Avec la puissance de calcul disponible maintenant, ce système est considéré incassable lorsque p a plus de 300 chiffres décimaux et k_1 et k_2 plus de 100 décimaux chiffres chacun.

SIGNATURES NUMÉRIQUES Non seulement la cryptographie peut être utilisée pour garantir la confidentialité des un message, mais il peut également être utilisé pour que le destinataire du message sache qu'il provient de la personne dont ils pensent que cela vient. Nous montrons d'abord comment un message peut être envoyé pour qu'un destinataire du message sera sûr que le message provient de l'expéditeur supposé du message.
En particulier, nous pouvons montrer comment cela peut être accompli en utilisant le cryptosystème RSA pour appliquer une **signature numérique** à un message.

Supposons que la clé publique RSA d'Alice soit (n, e) et que sa clé privée soit d . Alice crypte un simple SMS x utilisant la fonction de cryptage $E_{(n, e)}(x) = x^e$ **mod** n . Elle déchiffre un texte chiffré message y utilisant la fonction de déchiffrement $D_{(n, e)} = x^d$ **mod** n . Alice veut envoyer le message M pour que tous ceux qui reçoivent le message sachent qu'il est venu d'elle. Tout comme dans RSA cryption, elle traduit les lettres en leurs équivalents numériques et divise la chaîne résultante en blocs $m_1, m_2, ..., m_k$ tels que chaque bloc soit de la même taille qui soit le plus grand possible de sorte que $0 \leq m_i \leq n$ pour $i = 1, 2, ..., k$. Elle applique ensuite sa *fonction de décryptage* $D_{(n, e)}$ à chaque bloc, obtenant $D_{n, e}(m_i)$, $i = 1, 2, ..., k$. Elle envoie le résultat à tous les destinataires prévus du message.

Lorsqu'un destinataire reçoit son message, il applique la fonction de cryptage d'Alice $E_{(n, e)}$ à chaque bloc, dont tout le monde dispose, car la clé d'Alice (n, e) est une information publique. Le résultat est le bloc de texte en clair d'origine car $E_{(n, e)}(D_{(n, e)}(x)) = x$. Donc, Alice peut envoyer son message à autant de personnes qu'elle le souhaite et en le signant de cette manière, chaque destinataire peut être sûr qu'il est venu d'Alice. L'exemple 10 illustre ce protocole.

EXEMPLE 10 Supposons que la clé publique de cryptosystème RSA d'Alice soit la même que dans l'exemple 8. Autrement dit $n = 43 \cdot 59 = 2537$ et $e = 13$. Sa clé de déchiffrement est $d = 937$, comme décrit dans l'exemple 9. Elle veut envoyer le message «RENCONTREZ À MIDI» à ses amis afin qu'ils soient sûrs qu'il provienne de sa. Que doit-elle envoyer?

Solution: Alice traduit d'abord le message en blocs de chiffres, obtenant 1204 0419 0019 1314 1413 (comme le lecteur devrait vérifier). Elle applique ensuite sa transformation de décryptage $D_{(2537, 13)}(x) = x^{937}$ **mod** 2537 pour chaque bloc. En utilisant l'exponentiation modulaire rapide (avec le l'aide d'une aide au calcul), elle constate que 1204^{937} **mod** 2537 = 817, 419^{937} **mod** 2537 = 555, 19^{937} **mod** 2537 = 1310, 1314^{937} **mod** 2537 = 2173 et 1413^{937} **mod** 2537 = 1026.

Ainsi, le message qu'elle envoie, divisé en blocs, est 0817 0555 1310 2173 1026. Lorsque l'un des ses amis reçoivent ce message, ils appliquent sa transformation de chiffrement $E_{(2537, 13)}$ à chaque bloc. Quand ils le font, ils obtiennent les blocs de chiffres du message d'origine qu'ils traduisent retour aux lettres anglaises. ▲

Nous avons montré que les messages signés peuvent être envoyés à l'aide du cryptosystème RSA. Nous pouvons étendre ceci en envoyant des messages secrets signés. Pour ce faire, l'expéditeur applique le chiffrement RSA à l'aide de la clé de chiffrement connue du destinataire pour chaque bloc qui a été chiffré en utilisant la transformation de décryptage de l'expéditeur. Le destinataire applique alors d'abord son déchiffrement privé transformation, puis la transformation de cryptage public de l'expéditeur. (L'exercice 32 demande ce protocole à effectuer.)

Des exercices

1. Cryptez le message NE PAS PASSER EN TRADUISANT les lettres en chiffres, en appliquant le cryptage donné fonction, puis la traduction des chiffres en lettres ters.

a) $f(p) = (p + 3)$ **mod** 26 (le chiffre de César)
b) $f(p) = (p + 13)$ **mod** 26
c) $f(p) = (3p + 7)$ **mod** 26

2. Chiffrez le message STOP POLLUTION en traduisant les lettres en chiffres, en appliquant le cryptage donné fonction, puis la traduction des chiffres en lettres ters.

a) $f(p) = (p + 4)$ **mod** 26
b) $f(p) = (p + 21)$ **mod** 26
c) $f(p) = (17p + 22)$ **mod** 26

3. Chiffrez le message REGARDEZ VOTRE ÉTAPE en traduisant les lettres en chiffres, en appliquant le cryptage donné fonction de traduction, puis la conversion des nombres en des lettres.

a) $f(p) = (p + 14)$ **mod** 26
b) $f(p) = (14p + 21)$ **mod** 26
c) $f(p) = (-7p + 1)$ **mod** 26

4. Déchiffrez ces messages qui ont été chiffrés à l'aide du Chiffre César.

a) EOXH MHDQV
b) WHVW WRGDB
c) HDW GLP VXP

5. Déchiffrez ces messages chiffrés à l'aide du chiffre de décalage $f(p) = (p + 10)$ **mod** 26.

a) CEBBOXNOB XYG
b) LO WI PBSOXN
c) DSWO PYB PEX

6. Supposons que lorsqu'une longue chaîne de texte est chiffrée à l'aide un chiffre de décalage $f(p) = (p + k)$ **mod** 26, le plus courant lettre dans le texte chiffré est X. Quelle est la valeur la plus probable pour k *en* supposant que la distribution des lettres dans le texte est typique du texte anglais?

7. Supposons que lorsqu'une chaîne de texte anglais est cryptée, en utilisant un chiffre de décalage $f(p) = (p + k)$ **mod** 26, le résultat le texte chiffré est DY CVOOZ ZOBMRKXMO DY NBOKW. Quelle était la chaîne de texte en clair d'origine?

8. Supposons que le texte chiffré DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV a été pro- obtenu en chiffrant un message en clair à l'aide d'un décalage chiffrer. Qu'est-ce que le texte en clair d'origine?

9. Supposons que le texte chiffré ERC WYJJMGMIRXPC EHZERGIH XIGLRSPSKC MW MRHMWXM- RKYMWLEFPI JVSQ QEKMG a été produit par en- crypter un message en clair en utilisant un chiffre de décalage. Quel est le texte en clair original?

10. Déterminez s'il existe une clé pour laquelle le chiffrement fonction de chiffrement de décalage est la même que celle fonction de mise en sphère.

11. Quelle est la fonction de déchiffrement pour un chiffrement affine si le la fonction de cryptage est $c = (15p + 13)$ **mod** 26?

∗ **12.** Trouver toutes les paires de clés entières (a, b) pour les chiffrements affins pour dont la fonction de cryptage $c = (ap + b)$ **mod** 26 est identique à la fonction de décryptage correspondante.

13. Supposons que la lettre la plus courante et la seconde lettre la plus courante dans un long texte chiffré produit par chiffrement d'un texte en clair à l'aide d'un chiffrement affine $f(p) = (ap + b)$ **mod** 26 sont respectivement Z et J. Quels sont les les valeurs les plus probables de a et b ?

14. Crypter le message GRIZZLY BEARS à l'aide de blocs de cinq lettres et le chiffre de transposition basé sur la permutation de $\{1, 2, 3, 4, 5\}$ avec $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 1$, $\sigma(4) = 2$ et $\sigma(5) = 4$. Pour cet exercice, utilisez la lettre X autant de fois que nécessaire pour remplir la finale bloc de moins de cinq lettres.

15. Déchiffrez le message EABW EFRO ATMR ASIN qui est le texte chiffré produit en chiffrant un message en texte brut sauge utilisant le chiffre de transposition avec des blocs de quatre lettres et la permutation σ de $\{1, 2, 3, 4\}$ définie par $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$ et $\sigma(4) = 2$.

∗ **16.** Supposons que vous sachiez qu'un texte chiffré a été produit en chiffrant un message en clair avec une transposition chiffrer. Comment pourriez-vous vous y prendre pour la casser?

17. Supposons que vous ayez intercepté un message chiffré et lorsque vous déterminez la fréquence des lettres dans ce message sage, vous trouvez que les fréquences sont similaires à la fréquence de lettres en texte anglais. Quel type de chiffre pensez-vous a été utilisé?

Le **chiffre Vigenère** est un chiffre bloc, avec une clé qui est un chaîne de lettres avec des équivalents numériques $k_1 k_2 \ldots k_m$, où $k_i \in \mathbf{Z}_{26}$ pour $i = 1, 2, \ldots, m$. Supposons que le numérique les équivalents des lettres d'un bloc de texte en clair sont $p_1 p_2 \ldots p_m$. Le bloc de texte chiffré numérique correspondant est $(p_1 + k_1)$ **mod** 26 $(p_2 + k_2)$ **mod** 26 ... $(p_m + k_m)$ **mod** 26. Enfin, nous traduisons en lettres. Par exemple, supposons que le la chaîne de clé est ROUGE, avec des équivalents numériques 17 4 3. Ensuite, le texte en clair ORANGE, avec des équivalents numériques 14 17 00 13 06 04, est chiffré en le divisant d'abord en deux blocs 14 17 00 et 13 06 04. Ensuite, dans chaque bloc, nous déplaçons la première lettre par 17, la deuxième par 4 et la troisième par 3. Nous obtenir 5 21 03 et 04 10 07. Le cryptogramme est FVDEKH.

18. Utilisez le chiffrement Vigenère avec la clé BLEUE pour chiffrer message SNOWFALL.

19. Le texte chiffré OIKYWVHBX a été produit par cryptage un message en clair en utilisant le chiffrement Vigenère avec touche CHAUD. Qu'est-ce que le message en clair?

20. Exprimez le chiffre de Vigenère comme un cryptosystème.

Pour casser un chiffrement Vigenère en récupérant un message en clair le message chiffré sans avoir la clé, la première étape consiste à déterminer la longueur de la chaîne de clé. La deuxième étape consiste à comprendre chaque caractère de la chaîne de clé en déterminant la correspondance quart de travail. Les exercices 21 et 22 traitent de ces deux aspects.

21. Supposons que lorsqu'une longue chaîne de texte est chiffrée à l'aide un chiffre Vigenère, la même chaîne se trouve dans le texte chiffré à partir de plusieurs positions différentes. Expliquez comment ces informations Les informations peuvent être utilisées pour déterminer la longueur de la clé.

22. Une fois la longueur de la chaîne de clé d'un chiffre Vigènere connue, expliquer comment déterminer chacun de ses personnages. Suppose que le texte en clair est suffisamment long pour que la fréquence de sa est raisonnablement proche de la fréquence des lettres Texte en anglais.

∗ **23.** Montrer que l'on peut facilement factoriser n quand on sait que n est le produit de deux nombres premiers, p et q, et nous connaissons la valeur de $(p-1)(q-1)$.

Dans les exercices 24-27, exprimez d'abord vos réponses sans calculer exponentiations modulaires. Utilisez ensuite une aide au calcul pour compléter ces calculs.

24. Chiffrez le message ATTACK en utilisant le système RSA avec $n = 43 \cdot 59$ et $e = 13$, traduisant chaque lettre en nombres entiers et regrouper des paires d'entiers, comme dans l'exemple 8.

25. Crypter le message UPLOAD en utilisant le système RSA avec $n = 53 \cdot 61$ et $e = 17$, traduisant chaque lettre en nombres entiers et regrouper des paires d'entiers, comme dans l'exemple 8.

26. Quel est le message original chiffré à l'aide du système RSA avec $n = 53 \cdot 61$ et $e = 17$ si le message chiffré est 3185 2038 2460 2550? (Pour déchiffrer, trouvez d'abord le déchiffrement exposant d, qui est l'inverse de $e = 17$ modulo $52 \cdot 60$.)

27. Quel est le message d'origine chiffré à l'aide du système RSA avec $n = 43 \cdot 59$ et $e = 13$ si le message crypté est 0667 1947 0671? (Pour déchiffrer, recherchez d'abord l'exposant de déchiffrement d qui est l'inverse de $e = 13$ modulo $42 \cdot 58$.)

∗ **28.** Supposons que (n, e) est une clé de chiffrement RSA, avec $n = pq$ où p et q sont de grands nombres premiers et pgcd $(e, (p-1)(q-1)) = 1$. De plus, supposons que d est un inverse de e modulo $(p-1)(q-1)$. Supposer que $C \equiv M^e \pmod{pq}$. Dans le texte, nous avons montré que RSA Cryption, qui est, la congruence $C^d \equiv M \pmod{pq}$ détient lorsque gcd $(M, pq) = 1$. Montrer que cette congruence de décryptage est également valable lorsque gcd $(M, pq) > 1$. [*Astuce:* utilisez les congruences modulo p et modulo q et appliquer le reste chinois théorème.]

29. Décrire les étapes qu'Alice et Bob suivent lorsqu'ils utilisent le protocole d'échange de clés Diffie-Hellman pour générer un partage clé. Supposons qu'ils utilisent le premier $p = 23$ et prennent $a = 5$, qui est une racine primitive de 23, et qu'Alice sélectionne $k_1 = 8$ et Bob sélectionne $k_2 = 5$. (Vous voudrez peut-être utiliser l'aide internationale.)

30. Décrire les étapes qu'Alice et Bob suivent lorsqu'ils utilisent le protocole d'échange de clés Diffie-Hellman pour générer un partage clé. Supposons qu'ils utilisent le premier $p = 101$ et prennent $a = 2$, qui est une racine primitive de 101, et qu'Alice sélectionne $k_1 = 7$ et Bob sélectionne $k_2 = 9$. (Vous voudrez peut-être utiliser l'aide internationale.)

Dans les exercices 31 à 32, supposez qu'Alice et Bob ont ces clés publiques et clés privées correspondantes: $(n_{\text{Alice}}, e_{\text{Alice}}) = (2867, 7) = (61 \cdot 47, 7)$, $d_{\text{Alice}} = 1183$ et $(n_{\text{Bob}}, e_{\text{Bob}}) = (3127, 21) = (59 \cdot 53, 21)$, $d_{\text{Bob}} = 1149$. Exprimez d'abord votre swers sans effectuer les calculs. Ensuite, en utilisant une comsi elles sont disponibles, effectuez le calcul pour obtenir réponses numériques.

31. Alice veut envoyer à tous ses amis, y compris Bob, le messager sage "VENDRE TOUT" pour qu'il sache qu'elle a envoyé il. Que doit-elle envoyer à ses amis, en supposant qu'elle signe le message à l'aide du cryptosystème RSA.

32. Alice veut envoyer à Bob le message "ACHETER MAINTENANT" afin que il sait qu'elle l'a envoyé et que seul Bob peut le lire. Quoi devrait-elle envoyer à Bob, en supposant qu'elle signe le message et puis le crypte en utilisant la clé publique de Bob?

33. Nous décrivons un protocole d'échange de clé de base utilisant une clé privée cryptographie sur laquelle des protocoles plus sophistiqués pour l'échange de clés est basé. Le cryptage au sein du protocole est fait à l'aide d'un cryptosystème à clé privée (comme AES) qui est considéré comme sûr. Le protocole implique trois parties, Alice et Bob, qui souhaite échanger une clé, et un tiers de confiance Cathy. Supposons qu'Alice a une clé secrète k_{Alice} que seule elle et Cathy le savent, et Bob a une clé secrète k_{Bob} que lui seul et Cathy le savent. Le protocole comporte trois étapes:

(i) Alice envoie au tiers de confiance Cathy le message rechercher une clé partagée avec Bob »chiffrée à l'aide de la clé d'Alice k_{Alice}.

(ii) Cathy renvoie à Alice une clé $k_{\text{Alice, Bob}}$, qu'elle a généeffacé, chiffré à l'aide de la clé k_{Alice}, suivi de ce même clé $k_{\text{Alice, Bob}}$, chiffrée à l'aide de la clé de Bob, k_{Bob}.

(iii) Alice envoie à Bob la clé $k_{\text{Alice, Bob}}$ crypté à l'aide de k_{Bob}, connu seulement de Bob et de Cathy.

Expliquez pourquoi ce protocole permet à Alice et Bob de partager la clé secrète $k_{\text{Alice, Bob}}$, connue seulement d'eux et de Cathy.

Termes et résultats clés

TERMES

$a \mid b$ (a divise b): il y a un entier c tel que $b = ac$
a et b sont modulo congrus m : m divise $a - b$

arithmétique modulaire: arithmétique effectuée modulo un entier $m \geq 2$

premier: un entier supérieur à 1 avec exactement deux positifs diviseurs entiers

composite: un entier supérieur à 1 qui n'est pas premier

Mersenne prime: un premier de la forme $2^p - 1$, où p est premier

pgcd (a, b) (le plus grand commun diviseur de a et b): le plus grand entier qui divise à la fois a et b

entiers relativement premiers: entiers a et b tels que pgcd $(a, b) = 1$

entiers relativement premiers par paire: un ensemble d'entiers avec le propriété que chaque paire de ces entiers est relativement premier

ppcm (a, b) (le plus petit commun multiple de a et b): le plus petit entier positif divisible par a et b

a mod b : le reste lorsque l'entier a est divisé par le entier positif b

$a \equiv b$ (mod m) (a est congru avec b modulo m): $a - b$ est divisible par m

$n = (a_k a_{k-1} \ldots a_1 a_0)_b$: lareprésentation debase b de n

représentation binaire: la **représentation en** base 2 d'un entier

représentation octale: la **représentation en** base 8 d'un entier

représentation hexadécimale: la représentation en base 16 de un nombre entier

combinaison linéaire de a et b avec des coefficients entiers: an expression de la forme $sa + tb$, où s et t sont des entiers

Coefficients de Bézout de a et b : entiers s et t tels que le **L'identité de Bézout** $sa + tb =$ gcd (a, b) est valable

inverse d' *un* modulo m : un entier a tel que $aa \equiv 1 \pmod{m}$

congruence linéaire: une congruence de la forme $ax \equiv b \pmod{m}$, où x est une variable entière

pseudoprime à la base b : un entier composite n tel que $b^{n-1} \equiv 1 \pmod{n}$

Nombre de Carmichael: un entier composite n tel que n est un pseudoprime à la base b pour tous les entiers positifs b avec pgcd $(b, n) = 1$

racine primitive d'un premier p : un entier r dans $\mathbf{Z}_p$ tel que chaque entier non divisible par p est modulo congru p à une puissance de r

logarithme discret de a à la base r modulo p : l'entier e avec $0 \leq e \leq p - 1$ tel que $r^e \equiv a \pmod{p}$

cryptage: le processus de secret d'un message

décryptage: le processus de retour d'un message secret à son forme originale

clé de chiffrement: une valeur qui détermine laquelle d'une famille de les fonctions de cryptage doivent être utilisées

shift cipher: un chiffre qui chiffre la lettre en clair p comme $(p + k)$ **mod** m pour un entier k

chiffre affine: un chiffre qui chiffre la lettre en clair p comme $(ap + b)$ **mod** m pour les entiers a et b avec pgcd $(a, 26) = 1$

chiffre de caractère: un chiffre qui chiffre les caractères un par un

bloc de chiffrement: un chiffrement qui chiffre des blocs de caractères d'un taille fixe

crytanalyse: processus de récupération du texte en clair du texte sans connaître la méthode de chiffrement, ou connaissant la méthode de chiffrement, mais pas la clé

cryptosystème: un tuple à cinq (P, C, K, E, D) où P est l'ensemble des messages en clair, C est l'ensemble des messages chiffrés, K est l'ensemble des clés, E est l'ensemble des fonctions de cryptage, et D est l'ensemble des fonctions de déchiffrement

cryptage à clé privée: cryptage où les deux cryptages les clés et les clés de déchiffrement doivent être gardées secrètes

cryptage à clé publique: cryptage où se trouvent les clés de cryptage connaissance publique, mais les clés de déchiffrement sont gardées secrètes

Cryptosystème RSA: le cryptosystème où P et C sont les deux $\mathbf{Z}_{26}$, K est l'ensemble des paires $k = (n, e)$ où $n = pq$ où p et q sont de grands nombres premiers et e est un entier positif, $E_k(p) = p^e$ **mod** n , et $D_k(c) = c^d$ **mod** n où d est le inverse de e modulo $(p - 1)(q - 1)$

protocole d'échange de clés: un protocole utilisé par deux générer une clé partagée

signature numérique: une méthode qu'un destinataire peut utiliser pour le mien que l'expéditeur présumé d'un message réellement envoyé le message

RÉSULTATS

algorithme de division: Soit a et d *des* entiers avec d positif. Il existe alors des entiers uniques q et r avec $0 \leq r < d$ tels que $a = dq + r$.

Soit b un entier supérieur à 1. Alors si n est un pos- entier itif, il peut être exprimé uniquement sous la forme $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$.

L'algorithme pour trouver l' expansion de base b d'un entier (voir l'algorithme 1 à la section 4.2)

Les algorithmes conventionnels d'addition et de multiplication d'entiers (donné dans la section 4.2)

L'algorithme d'exponentiation modulaire (voir l'algorithme 5 dans Section 4.2)

Algorithme euclidien: pour trouver les plus grands diviseurs communs en utilisant successivement l'algorithme de division (voir Algorithme 1 dans la section 4.3)

Théorème de Bézout: si a et b sont des entiers positifs, alors Le pgcd (a, b) est une combinaison linéaire de a et b .

tamis d'Eratosthène: une procédure pour trouver tous les nombres premiers non dépassant un nombre spécifié n , décrit à la section 4.3

théorème fondamental de l'arithmétique: chaque entier positif peut être écrit uniquement comme le produit de nombres premiers, où le les facteurs premiers sont écrits par ordre croissant de taille.

Si a et b sont des entiers positifs, alors $ab =$ pgcd $(a, b) \cdot$ lcm (a, b) .

Si m est un entier positif et gcd $(a, m) = 1$, alors a a a modulo inverse unique m .

Théorème du reste chinois: un système de congruences linéaires les entiers relativement premiers modulo par paires ont une so- lution modulo le produit de ces modules.

Le petit théorème de Fermat: si p est premier et $p \mid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.

Questions de révision

1. Trouvez 210 **div** 17 et 210 **mod** 17.

2. a) Définissez ce que signifie que a et b soient des modèles congruents ulo 7.

b) Quelles paires des nombres entiers -11 , -8 , -7 , -1 , 0 , 3, et 17 sont modulo congruent 7?

c) Montrer que si a et b sont modulo 7 congruents, alors $10a + 13$ et $-4b + 20$ sont également modulo 7 congruents.

3. Montrer que si $a \equiv b \pmod{m}$ et $c \equiv d \pmod{m}$, alors $a + c \equiv b + d \pmod{m}$.

4. Décrire une procédure de conversion décimale (base 10) expansions d'entiers en expansions hexadécimales.

5. Convertissez $(1101\ 1001\ 0101\ 1011)_2$ en octal et hexadéci- représentations mal.

b) Exprimer le pgcd $(84, 119)$ comme une combinaison linéaire de 84 et 119.

11. a) Que signifie que a soit l'inverse de *un* modulo m ?

b) Comment trouver l'inverse d' *un* modulo m lorsque m est un entier positif et pgcd $(a, m) = 1$?

c) Trouvez un inverse de 7 modulo 19.

12. a) Comment l'inverse d' *un* modulo m peut-il être utilisé pour résoudre congruence $ax \equiv b \pmod{m}$ lorsque gcd $(a, m) = 1$?

b) Résolvez la congruence linéaire $7x \equiv 13 \pmod{19}$.

13. a) Énonce le théorème du reste chinois.

b) Trouver les solutions du système $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$ et $x \equiv 3 \pmod{7}$.

6. Convertissez $(7206)_8$ et $(A0EB)_{16}$ en une représentation binaire.

7. Énoncez le théorème fondamental de l'arithmétique.

8. a) Décrire une procédure pour trouver la factorisation tion d'un entier.
   b) Utilisez cette procédure pour trouver la factorisation 80.707.

9. a) Définissez le plus grand diviseur commun de deux entiers.
   b) Décrivez au moins trois façons différentes de trouver est le diviseur commun de deux nombres entiers. Quand est-ce que chacun méthode fonctionne le mieux?
   c) Trouver le plus grand commun diviseur de 1.234.567 et 7.654.321.
   d) Trouvez le plus grand commun diviseur de $2^3 3^5 5^7 7^9 11$ et $2^9 3^7 5^5 7^3 13$.

10. a) Comment trouver une combinaison linéaire (avec un entier coefficients) de deux entiers qui est égal à leur plus grand diviseur commun?

14. Supposons que $2^{n-1} \equiv 1 \pmod{n}$. N est-il nécessairement premier?

15. Utilisez le petit théorème de Fermat pour évaluer 9^{200} **mod** 19.

16. Expliquez comment le chiffre de contrôle est trouvé pour un ISBN à 10 chiffres.

17. Chiffrez le message POMMES ET ORANGES à l'aide d'un déplacer le chiffre avec la clé $k = 13$.

18. a) Quelle est la différence entre une clé publique et un système de cryptage à clé vate?
    b) Expliquez pourquoi l'utilisation de chiffres de décalage est un système de clé privée. tem.
    c) Expliquez pourquoi le cryptosystème RSA est une clé publique système.

19. Expliquez comment le cryptage et le décryptage sont effectués dans le Cryptosystème RSA.

20. Décrivez comment deux parties peuvent partager une clé secrète en utilisant Protocole d'échange de clés Diffie-Hellman.

Exercices supplémentaires

1. Le compteur kilométrique d'une voiture va jusqu'à 100 000 milles. le propriétaire actuel d'une voiture l'a achetée lorsque le compteur kilométrique a lu 43 179 milles. Il veut maintenant le vendre; quand vous examinez la voiture pour un achat éventuel, vous remarquez que ter lit 89 697 milles. Que pouvez-vous conclure sur la façon dont plusieurs miles, il a conduit la voiture, en supposant que le compteur kilométrique toujours fonctionné correctement?

2. a) Expliquez pourquoi n **div** 7 est égal au nombre de semaines en n jours.
   b) Expliquez pourquoi n **div** 24 est égal au nombre de jours en n heures.

3. Trouvez quatre nombres congrus à 5 modulo 17.

4. Montrez que si a et d sont des entiers positifs, alors il y a entiers q et r tels que $a = dq + r$ où $-d/2 < r \leq d/2$.

∗ 5. Montrer que si $ac \equiv bc \pmod{m}$, où a, b, c et m sont des entiers avec $m > 2$, et $d = \text{pgcd}(m, c)$, alors $a \equiv b \pmod{m/d}$.

6. Montrez que la somme des carrés de deux entiers impairs ne peut pas être le carré d'un entier.

7. Montrez que si $n^2 + 1$ est un carré parfait, où n est un entier, alors n est pair.

8. Démontrez qu'il n'y a pas de solution dans les entiers x et y pour l'équation $x^2 - 5y^2 = 2$. [*Astuce:* Considérez cette équation modulo 5.]

9. Développer un test de divisibilité d'un entier positif n par 8 basé sur l'expansion binaire de n.

10. Développer un test de divisibilité d'un entier positif n par 3 basé sur l'expansion binaire de n.

11. Concevoir un algorithme pour deviner un nombre entre 1 et $2^n - 1$ en devinant successivement chaque bit de son binaire expansion.

12. Déterminer la complexité, en termes de nombre de devine, nécessaire pour déterminer un nombre compris entre 1 et $2^n - 1$ en devinant successivement les bits dans son expansion.

13. Montrer qu'un entier est divisible par 9 si et seulement si le la somme de ses chiffres décimaux est divisible par 9.

∗∗ 14. Montrer que si a et b sont des nombres irrationnels positifs tels que que $1/a + 1/b = 1$, alors chaque entier positif peut être exprimée uniquement comme as $ka\rfloor$ ou $\lfloor kb \rfloor$ pour certains entier tive k.

15. Montrer qu'il existe une infinité de nombres premiers en montrant que $Q_n = n! + 1$ doit avoir un facteur premier supérieur à n chaque fois que n est un entier positif.

16. Trouvez un entier positif n pour lequel $Q_n = n! + 1$ n'est pas premier.

17. Utilisez le théorème de Dirichlet, qui déclare qu'il y a infiniment de nombreux nombres premiers dans chaque progression arithmétique $ak + b$ où gcd $(a, b) = 1$, pour montrer qu'il y a infiniment de nombreux nombres premiers qui se terminent par une expansion décimale avec un 1.

18. Montrer que si n est un entier positif tel que la somme de les diviseurs de n sont $n + 1$, alors n est premier.

∗ 19. Montrer que chaque entier supérieur à 11 est la somme de deux entiers composites.

20. Trouvez les cinq plus petits entiers composites consécutifs.

21. Montrer que la conjecture de Goldbach, qui déclare que toute un entier pair supérieur à 2 est la somme de deux nombres premiers, équivaut à la déclaration selon laquelle chaque entier supérieur que 5 est la somme de trois nombres premiers.

22. Trouver une progression arithmétique de longueur six commençant avec 7 qui ne contient que des nombres premiers.

∗ 23. Démontrer que si $f(x)$ est un polynôme non constant avec des coefficients plus élevés, alors il y a un entier y tel que $f(y)$ est composite. [*Astuce:* Supposons que $f(x_0) = p$ est premier. Spectacle que p divise $f(x_0 + kp)$ pour tous les entiers k. Obtenir une con-

30. Expliquez pourquoi vous ne pouvez pas directement adapter la preuve sont infiniment nombreux nombres premiers (théorème 3 de la section 4.3) à montrent qu'il existe une infinité de nombres premiers dans l'arith- progression metic $3k + 1$, $k\ 1 = , 2, \ldots$.

31. Expliquez pourquoi vous ne pouvez pas directement adapter la preuve sont infiniment nombreux nombres premiers (théorème 3 de la section 4.3) à montrent qu'il existe une infinité de nombres premiers dans l'arithmétique progression $4k + 1$, $k = 1, 2, \ldots$.

32. Montrer que si le plus petit facteur premier p du positif l'entier n est supérieur à $\sqrt[3]{n}$, alors n/p est premier ou égal à 1.

Un ensemble d'entiers est appelé **mutuellement relativement premier** si le le plus grand diviseur commun de ces entiers est 1.

33. Déterminez si les nombres entiers dans chacun de ces ensembles sont mutuellement relativement prime.

a) 8, 10, 12	**b)** 12, 15, 25
c) 15, 21, 28	**d)** 21, 24, 28, 32

34. Trouvez un ensemble de quatre entiers relativement premiers tels que que pas deux d'entre eux sont relativement premiers.

∗ 35. Pour lesquels les entiers positifs n sont $n^4 + 4^n$ premier?

36. Montrer que le système de congruences $x \equiv 2 \pmod{6}$ et $x \equiv 3 \pmod{9}$ n'a pas de solutions.

37. Trouver toutes les solutions du système de congruences $x \equiv 4 \pmod{6}$ et $x \equiv 13 \pmod{15}$.

∗ 38. a) Montrer que le système de congruences $x \equiv a_1 \pmod{m_1}$ et $x \equiv un_2 \pmod{m_2}$, où un_1, un_2, m_1, et m_2 sont entiers avec $m_1 > 0$ et $m_2 > 0$, a une solution si et seulement si pgcd $(m_1, m_2) \mid a_1 - a_2$.
   b) Montrer que si le système de la partie (a) a une solution, alors

tradition du fait qu'un polynôme de degré n , où $n > 1$, prend chaque valeur au maximum n fois.]

* **24.** Combien de zéros sont à la fin de l'expansion binaire de $100^{10!}$?

25. Utilisez l'algorithme euclidien pour trouver le plus grand commun diviseur de 10.223 et 33.341.

26. Combien de divisions sont nécessaires pour trouver un pgcd $(144, 233)$ en utilisant l'algorithme euclidien?

27. Trouvez pgcd $(2n+1, 3n+2)$, où n est un entier positif. [*Astuce:* utilisez l'algorithme euclidien.]

28. **a)** Montrer que si a et b sont des entiers positifs gers avec $a \geq b$, alors gcd $(a, b) = a$ si $a = b$, pgcd $(a, b) = 2$ pgcd $(a/2, b/2)$ si a et b sont pairs, pgcd $(a, b) =$ pgcd $(a/2, b)$ si a est pair et b est impair, et pgcd $(a, b) =$ pgcd $(a - b, b)$ si a et b sont tous deux impairs.

b) Expliquez comment utiliser (a) pour construire un algorithme pour calcul du plus grand diviseur commun de deux positions nombres entiers qui n'utilisent que des comparaisons, des soustractions, et les décalages des extensions binaires, sans utiliser divisions.

c) Trouvez gcd $(1202, 4848)$ *en* utilisant cet algorithme.

29. Adapter la preuve qu'il existe une infinité de nombres premiers (Theorem 3 dans la section 4.3) pour montrer qu'il y a une infinité de les nombres premiers dans la progression arithmétique $6k + 5$, $k = 1, 2, \ldots$

c'est un modulo lcm unique (m_1, m_2) .

39. Montrer que 30 divise $n^9 - n$ pour chaque non négatif entier n .

40. Montrer que $n^{12} - 1$ est divisible par 35 pour chaque entier n pour lequel pgcd $(n, 35) = 1$.

41. Montrer que si p et q sont des nombres premiers distincts, alors $p^{q-1} + q^{p-1} -1$ (1 (mod pq).

Le chiffre de contrôle a_{13} pour un ISBN-13 avec les premiers chiffres $a_1 a_2 \ldots a_{12}$ est déterminé par la congruence $(a_1 + a_3 + \cdots + a_{13}) + 3(a_2 + a_4 + \cdots + a_{12}) \equiv 0 \pmod{10}$.

42. Déterminez si chacun de ces nombres à 13 chiffres est un ISBN-13 valide.

a) 978-0-073-20679-1

b) 978-0-45424-521-1

c) 978-3-16-148410-0

d) 978-0-201-10179-9

43. Montrer que le chiffre de contrôle d'un ISBN-13 peut toujours détecter une seule erreur.

44. Montrez qu'il existe des transpositions de deux chiffres qui sont non détecté par un ISBN-13.

Un **numéro de transit de routage (RTN)** est un code bancaire utilisé dans les États-Unis qui figurent au bas des chèques. La forme la plus courante d'un RTN comporte neuf chiffres, où le dernier chiffre est un chiffre de contrôle. Si $d_1 d_2 \ldots d_9$ est un RTN valide,

la congruence $3(d_1 + d_4 + d_7) + 7(d_2 + d_5 + d_8) + (d_3 + d_6 + d_9) \equiv 0 \pmod{10}$ doit tenir.

45. Montrer que si $d_1 d_2 \ldots d_9$ est un RTN valide, alors $d_9 = 7(d_1 + d_4 + d_7) + 3(d_2 + d_5 + d_8) + 9(d_3 + d_6)$ **mod** 10. Furthermore, utilisez cette formule pour trouver le chiffre de contrôle qui suit les huit chiffres 11100002 dans un RTN valide.

46. Montrer que le chiffre de contrôle d'un RTN peut détecter tous les erreurs et déterminer quelles erreurs de transposition un RTN le chiffre de contrôle peut attraper et ceux qu'il ne peut pas attraper.

47. La version cryptée d'un message est LJMKG MGMXF QEXMW. S'il a été chiffré à l'aide de la pher $f(p) = (7p + 10)$ **mod** 26, quel était l'original message?

Chiffrements autokey sont chiffrements où la n ième lettre du Plainle texte est décalé de l'équivalent numérique de la n ème lettre de un flux de clés. Le flux de clés commence par une lettre de départ; son sousles lettres successives sont construites en utilisant soit le texte en clair soit le texte chiffré. Lorsque le texte en clair est utilisé, chaque caractère du keystream, après la première, est la lettre précédente du texte en clair. Lorsque le texte chiffré est utilisé, chaque caractère suivant du keystream, après la première, est la lettre précédente du texte chiffré calculé jusqu'à présent. Dans les deux cas, les lettres en clair sont cryptées en décalant chaque caractère de l'équivalent numérique du lettre clé correspondante.

48. Utilisez le chiffrement autokey pour crypter le message MAINTENANT EST LE TEMPS DE DÉCIDER (en ignorant les espaces) en utilisant

a) le flux de clés avec la graine X suivi des lettres du texte en clair.

b) le flux de clés avec la graine X suivi des lettres du texte chiffré.

49. Utilisez le chiffrement autokey pour crypter le message RÊVE DE RAISON (en ignorant les espaces) en utilisant

a) le flux de clés avec la graine X suivi des lettres du texte en clair.

b) le flux de clés avec la graine X suivi des lettres du texte chiffré.

Projets informatiques

Écrivez des programmes avec ces entrées et sorties.

1. Étant donné les entiers n et b , chacun supérieur à 1, trouvez la base b expansion de cet entier.

2. Étant donné les entiers positifs a, b et m avec $m > 1$, trouver a^b **mod** m .

3. Etant donné un entier positif, trouvez l'expansion de Cantor de cette entier (voir le préambule de l'exercice 48 de la section 4.2).

4. Étant donné un entier positif, déterminez s'il est premier en utilisant la division d'essai.

5. Étant donné un entier positif, trouver la factorisation principale de cet entier.

6. Étant donné deux nombres entiers positifs, trouvez leur plus grand commun diviseur utilisant l'algorithme euclidien.

7. Étant donné deux nombres entiers positifs, trouvez leur multiplicité la moins commune. tiple.

8. Étant donné les entiers positifs a et b , trouvez les coefficients de Bézout s et t de a et b .

9. Étant donné des entiers positifs relativement premiers a et b , trouver un inverse d' *un* modulo b .

10. Étant donné n congruences linéaires modulo par paires relativement modules principaux, trouver la solution simultanée de ces con-

14. Étant donné un message et un entier positif k inférieur à 26, crypter ce message en utilisant le chiffre de décalage avec la clé k ; et étant donné un message chiffré à l'aide d'un chiffre de décalage avec clé k , déchiffrez ce message.

15. Étant donné un message et des entiers positifs a et b inférieurs à 26 avec gcd $(a, 26)$, crypter ce message en utilisant une affine chiffrer avec la clé (a, b) ; et donné un message crypté usen utilisant le chiffre affine avec la clé (a, b) , déchiffrez ce message, en trouvant d'abord la clé de déchiffrement, puis en appliquant le transformation de décryptage appropriée.

16. Recherchez le message en texte brut d'origine à partir du texte chiffré message produit en chiffrant le message en clair en utilisant un chiffre de décalage. Pour ce faire, en utilisant un nombre de fréquences de lettres dans le texte chiffré.

* **17.** Construisez une clé de chiffrement RSA valide en en trouvant deux amorce p et q avec 200 chiffres chacun et un entier $e > 1$ relativement premier à $(p-1)(q-1)$.

18. Étant donné un message et un entier $n = pq$ où p et q sont des nombres premiers impairs et un entier $e > 1$ relativement premier à $(p-1)(q-1)$, crypter le message à l'aide du RSA cryptosystème avec clé (n, e) .

gruences modulo le produit de ces modules.

11. Étant donné un entier positif N, un module m, un multiplicateur a, un incrément c, et une graine x_0, où $0 \leq a < m$, $0 \leq c < m$, et $0 \leq x_0 < m$, génèrent la séquence de N pseudo-nombres aléatoires utilisant le générateur congruentiel linéaire $x_{n+1} = (ax_n + c)$ **mod** m.

12. Étant donné un ensemble de numéros d'identification, utilisez une fonction de hachage pour les affecter à des emplacements de mémoire où k emplacements de mémoire.

13. Calculez le chiffre de contrôle lorsque les neuf premiers chiffres sont donnés d'un ISBN-10.

19. Étant donné une clé RSA valide (n, e), et les nombres premiers p et q avec $n = pq$, trouver la clé de déchiffrement associée d.

20. Étant donné un message chiffré à l'aide du cryptosystème RSA avec la clé (n, e) et la clé de déchiffrement associée d, crypte ce message.

21. Générez une clé partagée à l'aide de la clé Diffie-Hellman changer le protocole.

22. Compte tenu des clés publiques et privées RSA de deux parties, envoyer un message secret signé de l'une des parties à L'autre.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Déterminez si $2^p - 1$ est premier pour chacun des nombres premiers n'excédant pas 100.

2. Testez une gamme de grands nombres de Mersenne $2^p - 1$ à dé-déterminer s'ils sont premiers. (Vous voudrez peut-être utiliser logiciel du projet GIMPS.)

3. Déterminer si $Q_n = p_1 p_2 \cdots p_n + 1$ est premier où $p_1, p_2, \ldots, p_n$ sont les n plus petits nombres premiers, pour as autant d'entiers positifs n que possible.

4. Recherchez des polynômes dans une variable dont les valeurs à les longues séries d'entiers consécutifs sont toutes des nombres premiers.

5. Trouver autant de nombres premiers de la forme $n^2 + 1$ où n est un pos-entier itif que vous pouvez. On ne sait pas s'il existe infiniment de tels nombres premiers.

6. Trouvez 10 nombres premiers différents chacun avec 100 chiffres.

7. Combien de nombres premiers y a-t-il moins de 1 000 000, moins de 10 000 000 et moins de 100 000 000? Pouvez-vous proposer une estimation du nombre de nombres premiers inférieurs à x où x est un entier positif?

8. Trouvez un facteur premier de chacun des 10 chiffres différents de 20 chiffres impairs entiers, sélectionnés au hasard. Gardez une trace de combien de temps prend pour trouver un facteur de chacun de ces entiers. Faites le même chose pour 10 entiers impairs différents à 30 chiffres, 10 différents entiers impairs à 40 chiffres, et ainsi de suite, tant que que possible.

9. Trouvez tous les pseudoprimes à la base 2 qui ne dépassent pas 10 000.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Décrivez le test de Lucas – Lehmer pour déterminer si un nombre de Mersenne est premier. Discutez des progrès de la Projet GIMPS pour trouver des nombres premiers de Mersenne à l'aide de ce test.

2. Expliquez comment les tests de primalité probabilistes sont utilisés de produire des nombres extrêmement importants qui sont presque certainement premier. Ces tests ont-ils un potentiel dos?

3. La question de savoir s'il existe une infinité de Le nombre de Carmichael a été résolu récemment après avoir été ouvert depuis plus de 75 ans. Décrivez les ingrédients dans la preuve qu'il existe une infinité de tels nombres.

4. Résumez l'état actuel des algorithmes de factorisation dans en termes de leur complexité et la taille des nombres qui peuvent actuellement pris en compte. Quand pensez-vous que ce sera possible de factoriser des nombres à 200 chiffres?

5. Décrire les algorithmes actuellement utilisés par les modernes ordinateurs pour additionner, soustraire, multiplier et diviser positif entiers.

6. Décrivez l'histoire du théorème du reste chinois. Décrivez certains des problèmes pertinents posés par écrits nus et hindous et comment le reste chinois le théorème s'applique à eux.

7. Quand les nombres d'une séquence sont-ils vraiment des nombres aléatoires? bers, et non pseudo-aléatoire? Quelles sont les lacunes été observé dans des simulations et des expériences dans lesquelles des nombres pseudo-aléatoires ont-ils été utilisés? Quels sont les propriétés que les nombres pseudo-aléatoires peuvent avoir les numéros de dom ne devraient pas avoir?

8. Expliquez comment un chiffre de contrôle est trouvé pour un Numéro de compte bancaire (IBAN) et discuter des types de les erreurs qui peuvent être trouvées en utilisant ce chiffre de contrôle.

9. Décrire l'algorithme de Luhn pour trouver le chiffre de contrôle d'un numéro de carte de crédit et discuter des types d'erreurs qui peut être trouvé en utilisant ce chiffre de contrôle.

10. Montrez comment une congruence peut être utilisée pour dire le jour de semaine pour une date donnée.

11. Décrivez comment la cryptographie à clé publique est appliquée. Les modalités d'application sont-elles sûres compte tenu du statut algorithmes de toring? Les informations seront-elles protégées en utilisant la cryptographie à clé publique devient-elle précaire à l'avenir?

12. Décrire comment la cryptographie à clé publique peut être utilisée pour produire des messages secrets signés afin que le destinataire soit relativement sûr que le message a été envoyé par la personne soupçonné de l'avoir envoyé.

13. Décrire le cryptosystème à clé publique Rabin, en expliquant comment chiffrer et comment déchiffrer les messages et pourquoi peut être utilisé comme système de cryptage à clé publique.

∗ **14.** Expliquez pourquoi il ne serait pas approprié d'utiliser p, où p est un grand premier, car le module de chiffrement dans le Cryptosystème RSA. Autrement dit, expliquez comment quelqu'un pourrait, sans calcul excessif, trouvez une clé privée dans la clé publique correspondante si le module était un grand premier, plutôt que le produit de deux grands nombres premiers.

15. Expliquez ce que signifie une fonction de hachage cryptographique? Quelles sont les propriétés importantes d'une telle fonction avoir?

CHAPITRE

Induction et récursivité

De nombreux énoncés mathématiques affirment qu'une propriété est vraie pour tous les entiers positifs. Des exemples de telles déclarations sont que pour chaque entier positif n : $n! \leq n^n$, $n^3 - n$ est divisible par 3; un ensemble avec n éléments a 2^n sous-ensembles; et la somme des n premiers entiers positifs est $n(n+1)/2$. L'un des principaux objectifs de ce chapitre et du livre est de donner à l'étudiant une compréhension de l'induction mathématique, qui est utilisée pour prouver des résultats de ce type.

Les épreuves utilisant l'induction mathématique comportent deux parties. Tout d'abord, ils montrent que la déclaration vaut pour l'entier positif 1. Deuxièmement, ils montrent que si la déclaration vaut pour un positif entier, il doit également tenir pour le prochain entier plus grand. L'induction mathématique est basée sur règle d'inférence qui nous dit que si $P(1)$ et $\forall k\,(P(k) \rightarrow P(k+1))$ sont vrais pour le domaine de entiers positifs, alors $\forall n P(n)$ est vrai. L'induction mathématique peut être utilisée pour prouver variété de résultats. Comprendre comment lire et construire des preuves par induction mathématique est un objectif clé de l'apprentissage des mathématiques discrètes.

Dans le chapitre 2, nous avons explicitement défini des ensembles et des fonctions. Autrement dit, nous avons décrit les ensembles en énumérant leurs éléments ou en donnant une propriété qui caractérise ces éléments. Nous avons donné des formules pour les valeurs des fonctions. Il existe un autre moyen important de définir de tels objets, basé sur Induction mathematique. Pour définir des fonctions, certains termes initiaux sont spécifiés et une règle est donné pour trouver des valeurs ultérieures à partir de valeurs déjà connues. (Nous avons brièvement abordé cette sorte de définition dans le chapitre 2 lorsque nous avons montré comment les séquences peuvent être définies en utilisant la récurrence Les ensembles peuvent être définis en listant certains de leurs éléments et en donnant des règles de construction éléments de ceux déjà connus pour être dans l'ensemble. Ces définitions, appelées *définitions récursives,* sont utilisés dans les mathématiques discrètes et l'informatique. Une fois que nous avons défini un ensemble récursivement, nous pouvons utiliser une méthode de preuve appelée induction structurelle pour prouver les résultats sur cet ensemble.

Lorsqu'une procédure est spécifiée pour résoudre un problème, cette procédure doit *toujours* résoudre le problème correctement. Il suffit de tester pour voir que le résultat correct est obtenu pour un ensemble d'entrées Les valeurs ne montrent pas que la procédure fonctionne toujours correctement. La justesse d'une procédure ne peut être garanti qu'en prouvant qu'il donne toujours le bon résultat. La dernière section de ce chapitre contient une introduction aux techniques de vérification de programme. Ceci est un formel technique pour vérifier que les procédures sont correctes. La vérification du programme sert de base à tentatives en cours pour prouver de façon mécanique que les programmes sont corrects.

Induction mathématique

introduction

Supposons que nous ayons une échelle infinie, comme le montre la figure 1, et nous voulons savoir si nous pouvons atteindre chaque étape sur cette échelle. Nous savons deux choses:

1. Nous pouvons atteindre le premier échelon de l'échelle.
2. Si nous pouvons atteindre un échelon particulier de l'échelle, alors nous pouvons atteindre l'échelon suivant.

Pouvons-nous conclure que nous pouvons atteindre chaque échelon? Par (1), nous savons que nous pouvons atteindre le premier barreau de l'échelle. De plus, parce que nous pouvons atteindre le premier échelon, par (2), nous pouvons également atteindre le deuxième échelon; c'est l'échelon suivant après le premier échelon. Appliquer à nouveau (2), car nous pouvons atteindre le deuxième échelon, nous pouvons également atteindre le troisième échelon. Poursuivant ainsi, nous pouvons montrer que nous

……

On peut atteindre l'étape $k + 1$ si
nous pouvons atteindre l'étape k

Étape $k + 1$
Étape k

Étape 4
Étape 3
Nous pouvons atteindre
étape 1
Étape 2
Étape 1

FIGURE 1 **Monter une échelle infinie.**

peut atteindre le quatrième échelon, le cinquième échelon, etc.Par exemple, après 100 utilisations de (2), nous savons que nous pouvons atteindre le 101e échelon. Mais pouvons-nous conclure que nous sommes en mesure d'atteindre chaque échelon de cette échelle infinie? La réponse est oui, quelque chose que nous pouvons vérifier en utilisant une preuve importante technique appelée **induction mathématique** . Autrement dit, nous pouvons montrer que *P (n)* est vrai pour chaque entier positif *n* , où *P (n)* est l'énoncé selon lequel nous pouvons atteindre le*n* ème échelon de l'échelle.

L'induction mathématique est une technique de preuve extrêmement importante qui peut être utilisée pour prouver assertions de ce type. Comme nous le verrons dans cette section et dans les sections suivantes de ce chapitre et les chapitres suivants, l'induction mathématique est largement utilisée pour prouver les résultats variété d'objets discrets. Par exemple, il est utilisé pour prouver des résultats sur la complexité de algorithmes, la justesse de certains types de programmes informatiques, les théorèmes sur les graphiques et arbres, ainsi qu'un large éventail d'identités et d'inégalités.

Dans cette section, nous décrirons comment l'induction mathématique peut être utilisée et pourquoi technique de preuve valide. Il est extrêmement important de noter que l'induction mathématique peut être utilisée seulement pour prouver les résultats obtenus d'une autre manière.Ce n'est *pas* un outil pour découvrir des formules ou théorèmes.

Induction mathematique

En général, l'induction mathématique * peut être utilisé pour prouver des déclarations qui affirment que*P (n)* est vrai pour tous les entiers positifs *n* , où *P (n)* est une fonction propositionnelle. Une preuve mathématique

* Malheureusement, l'utilisation de la terminologie «induction mathématique» se heurte à la terminologie utilisée pour décrire différents types de raisonnement. En logique, **le raisonnement déductif** utilise des règles d'inférence pour tirer des conclusions des prémisses, tandis que l'**induction le raisonnement** fait que les conclusions ne sont étayées, mais pas garanties, par des preuvesPreuves mathématiques, y compris les arguments utilisent l'induction mathématique, sont déductives et non inductives.

l'induction a deux parties, une **étape de base** , où nous montrons que $P(1)$ est vraie, et une **étape inductive** , où nous montrons que pour tous les entiers positifs k , si $P(k)$ est vrai, alors $P(k+1)$ est vrai.

PRINCIPE DE L'INDUCTION MATHÉMATIQUE Prouver que $P(n)$ est vrai pour tous entiers positifs n , où $P(n)$ est une fonction propositionnelle, nous effectuons deux étapes:

ÉTAPE DE BASE: Nous vérifions que $P(1)$ est vrai.

ÉTAPE INDUCTIVE: Nous montrons que l'énoncé conditionnel $P(k) \to P(k+1)$ est vrai pour tous les entiers positifs k .

Pour compléter l'étape inductive d'une preuve en utilisant le principe de l'induction mathématique, nous supposons que $P(k)$ est vrai pour un entier positif arbitraire k et montrons que dans cette hypothèse, $P(k+1)$ doit également être vrai. L'hypothèse que $P(k)$ est vraie est appelée l' **hypothèse inductive** .

Une fois que nous avons terminé les deux étapes d'une preuve par induction mathématique, nous avons montré que $P(n)$ est vrai pour tous les entiers positifs, c'est-à-dire que nous avons montré que $\forall n P(n)$ est vrai où la quantification est sur l'ensemble des entiers positifs. Dans l'étape inductive, nous montrons que $\forall k (P(k) \to P(k+1))$ est vrai, là encore, le domaine est l'ensemble des entiers positifs.

Exprimée comme une règle d'inférence, cette technique de preuve peut être déclarée comme

$$(P(1) \wedge \forall k (P(k) \to P(k+1))) \to \forall n P(n),$$

lorsque le domaine est l'ensemble des entiers positifs. Parce que l'induction mathématique est un technique importante, il vaut la peine d'expliquer en détail les étapes d'une épreuve utilisant cette technique. La première chose que nous faisons pour prouver que $P(n)$ est vrai pour tous les entiers positifs n est de montrer que $P(1)$ est vrai. Cela revient à montrer que la déclaration particulière obtenue lorsque n est remplacé par 1 dans $P(n)$ est vrai. Ensuite, nous devons montrer que $P(k) \to P(k+1)$ est vrai pour chaque entier positif k . À prouver que cette déclaration conditionnelle est vraie pour chaque entier positif k , nous devons montrer que $P(k+1)$ ne peut pas être faux lorsque $P(k)$ est vrai. Cela peut être accompli en supposant que $P(k)$ est vrai et montre que *sous cette hypothèse* $P(k+1)$ doit également être vrai.

Remarque: Dans une preuve par induction mathématique, on *ne* suppose *pas* que $P(k)$ soit vrai pour tout positif des entiers! On montre seulement que *si l'on suppose* que $P(k)$ est vrai, alors $P(k+1)$ est également vrai. Donc, une preuve par induction mathématique n'est pas un cas de mendicité ou de raisonnement circulaire.

Lorsque nous utilisons l'induction mathématique pour prouver un théorème, nous montrons d'abord que $P(1)$ est vrai. alors nous savons que $P(2)$ est vrai, car $P(1)$ implique $P(2)$. De plus, nous savons que $P(3)$ est vrai, parce que $P(2)$ implique $P(3)$. En poursuivant dans cette voie, nous voyons que $P(n)$ est vrai pour chaque entier positif n .

NOTE HISTORIQUE La première utilisation connue de l'induction mathématique est dans les travaux du XVIe siècle le mathématicien Francesco Maurolico (1494-1575). Maurolico a beaucoup écrit sur les œuvres du classique mathématiques et fait de nombreuses contributions à la géométrie et l'optique. Dans son livre *Arithmeticorum Libri Duo,* Maurolico a présenté une variété de propriétés des entiers ainsi que des preuves de ces propriétés. Prouver certaines de ces propriétés, il a conçu la méthode d'induction mathématique. Sa première utilisation de mathématiques L'induction dans ce livre devait prouver que la somme des n premiers entiers positifs impairs est égale à n^2 . Augustus De Morgan est crédité de la première présentation en 1838 de preuves formelles utilisant l'induction mathématique, ainsi comme introduisant la terminologie «induction mathématique». Les preuves de Maurolico étaient informelles et il n'a jamais utilisé le mot «induction». Voir [Gu11] pour en savoir plus sur l'histoire de la méthode d'induction mathématique.

FIGURE 2 **Illustrant le fonctionnement de l'induction mathématique à l'aide de dominos.**

FAÇONS DE RETENIR COMMENT FONCTIONNE INDUCTION MATHÉMATIQUES **Vous** songez à l'échelle infinie et les règles pour atteindre les étapes peuvent vous aider à vous rappeler comment les mathématiques travaux d'induction. Notez que les instructions (1) et (2) pour l'échelle infinie sont exactement la base étape et étape inductive, respectivement, de la preuve que $P(n)$ est vrai pour tous les entiers positifs n, où $P(n)$ est l'affirmation selon laquelle nous pouvons atteindre le n ème échelon de l'échelle. Par conséquent, nous pouvons invoquer l'induction mathématique pour conclure que nous pouvons atteindre chaque échelon.

Une autre façon d'illustrer le principe de l'induction mathématique est de considérer un infini rangée de dominos, étiquetés $1, 2, 3, \ldots, n, \ldots$, où chaque domino est debout. Soit $P(n)$ soit la proposition que domino n est renversé. Si le premier domino est renversé, c'est-à-dire si $P(1)$ est vrai - et si, chaque fois que le k ème domino est renversé, il frappe également le $(k + 1)$ st domino plus - c'est-à-dire si $P(k) \rightarrow P(k + 1)$ est vrai pour tous les entiers positifs k - alors tous les dominos sont renversé. Ceci est illustré sur la figure 2.

Pourquoi l'induction mathématique est valide

Pourquoi l'induction mathématique est-elle une technique de preuve valide? La raison vient du bien-propriété de classement, énumérée à l'annexe 1, en tant qu'axiome pour l'ensemble des entiers positifs, qui indique que chaque sous-ensemble non vide de l'ensemble d'entiers positifs a un moindre élément. Alors supposez nous savons que $P(1)$ est vrai et que la proposition $P(k) \rightarrow P(k + 1)$ est vraie pour tout positif entiers k. Pour montrer que $P(n)$ doit être vrai pour tous les entiers positifs n, supposons qu'il y ait à au moins un entier positif pour lequel $P(n)$ est faux. Ensuite, l'ensemble S d'entiers positifs pour lesquels $P(n)$ est faux est non vide. Ainsi, par la propriété bien ordonnée, S a un moindre élément, qui sera désigné par m. Nous savons que m ne peut pas être 1, car $P(1)$ est vrai. Parce que m est positif et supérieur à 1, $m - 1$ est un entier positif. De plus, comme $m - 1$ est inférieur à m, il est pas dans S, donc $P(m - 1)$ doit être vrai. Parce que l'instruction conditionnelle $P(m - 1) \rightarrow P(m)$ est également vrai, il faut que $P(m)$ soit vrai. Cela contredit le choix de m. Par conséquent, $P(n)$ doit être vrai pour chaque entier positif n.

Le bien et le mal de l'induction mathématique

Un point important doit être fait au sujet de l'induction mathématique avant de commencer un étude de son utilisation. La bonne chose à propos de l'induction mathématique est qu'elle peut être utilisée pour prouver

Vous pouvez prouver un théorème de mathématique induction même si tu le fais pas le moindre idée pourquoi c'est vrai!

une conjecture une fois qu'elle est faite (et c'est vrai). La mauvaise chose à ce sujet est qu'il ne peut pas être utilisé pour trouver de nouveaux théorèmes. Les mathématiciens trouvent parfois des preuves par des production insatisfaisante car elle ne permet pas de comprendre pourquoi les théorèmes sont vrais. Beaucoup les théorèmes peuvent être prouvés de plusieurs façons, y compris par induction mathématique. Les preuves de ces thé-orems par des méthodes autres que l'induction mathématique sont souvent préférés en raison de la perspicacité ils apportent.

Exemples de preuves par induction mathématique

De nombreux théorèmes affirment que $P(n)$ est vrai pour tous les entiers positifs n, où $P(n)$ est une propositionnelle une fonction. L'induction mathématique est une technique pour prouver des théorèmes de ce type. En d'autres termes, l'induction mathématique peut être utilisée pour prouver des énoncés de la forme $\forall n\ P(n)$, où le domaine est l'ensemble des entiers positifs. L'induction mathématique peut être utilisée pour prouver une variété de théorèmes, dont chacun est une déclaration de cette forme.(Rappelez-vous, beaucoup de mathématiques les assertions incluent un quantificateur universel implicite. L'énoncé «si n est un entier positif, alors $n^3 - n$ est divisible par 3 "en est un exemple. Rendre explicite le quantificateur universel implicite donne l'énoncé «pour tout entier positif n , $n^3 - n$ est divisible par 3.)

Nous utiliserons la façon dont les théorèmes sont prouvés en utilisant l'induction mathématique. Les théorèmes que nous allons prouver inclure les formules de sommation, les inégalités, les identités pour les combinaisons d'ensembles, la divisibilité résultats, théorèmes sur les algorithmes et quelques autres résultats créatifs. Dans cette section et plus tard sections, nous allons utiliser l'induction mathématique pour prouver de nombreux autres types de résultats, y compris l'exactitude des programmes informatiques et des algorithmes. L'induction mathématique peut être utilisée pour prouver une grande variété de théorèmes, pas seulement des formules de sommation, des inégalités et d'autres types de exemples que nous illustrons ici. (Pour les preuves par induction mathématique de beaucoup plus intéressantes et des résultats divers, voir le *Handbook of Mathematical Induction* de David Gunderson [Gu11]. Ce livre fait partie de la vaste série CRC en mathématiques discrètes, dont beaucoup peuvent être d'intérêt pour les lecteurs. L'auteur est l'éditeur de la série de ces livres).

Notez qu'il existe de nombreuses possibilités d'erreurs dans les épreuves à induction. Nous décrirons certains preuves incorrectes par induction mathématique à la fin de cette section et dans les exercices. À éviter de faire des erreurs dans les épreuves par induction mathématique, essayez de suivre les preuves fournies à la fin de cette section.

Cherchez le IH = symbole à voir où l'inductif l'hypothèse est utilisée.

VOIR OER L'HYPOTHÈSE INDUCTIVE EST UTILISÉE Pour aider le lecteur à comprendre chacune des preuves mathématiques d'induction dans cette section, nous noterons où l'inductif l'hypothèse est utilisée. Nous indiquons cette utilisation de trois manières différentes: par mention explicite dans le texte, en insérant l'acronyme IH (pour hypothèse inductive) sur un signe égal ou un signe pour un l'inégalité, ou en spécifiant l'hypothèse inductive comme la raison d'une étape dans une multi-ligne afficher.

FOURNIR DES FORMULES DE SOMMATION Nous commençons par utiliser l'induction mathématique pour plusieurs formules de sommation. Comme nous le verrons, l'induction mathématique est particulièrement bien adaptée pour prouver que ces formules sont valides. Cependant, les formules de sommation peuvent être prouvées dans d'autres façons. Cela n'est pas surprenant car il existe souvent différentes façons de prouver un théorème. Le principal l'inconvénient d'utiliser l'induction mathématique pour prouver une formule de sommation est que vous ne pouvez pas l'utiliser pour dériver cette formule. Autrement dit, vous devez déjà avoir la formule avant d'essayer de le prouver par induction mathématique.

Les exemples 1 à 4 illustrent comment utiliser l'induction mathématique pour prouver des formules de sommation. La première formule de sommation que nous prouverons par induction mathématique, dans l'exemple 1, est un formule pour la somme des plus petits n entiers positifs.

EXEMPLE 1 Montrer que si n est un entier positif, alors

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Solution: Soit $P(n)$ la proposition selon laquelle la somme des n premiers entiers positifs, $1 + 2 + \cdots n = \frac{n(n+1)}{2}$, est $n(n+1)/2$. Nous devons faire deux choses pour prouver que $P(n)$ est vrai pour $n = 1, 2, 3, \ldots$. À savoir, nous devons montrer que $P(1)$ est vrai et que l'énoncé conditionnel $P(k)$ implique $P(k+1)$ est vrai pour $k = 1, 2, 3, \ldots$.

ÉTAPE DE BASE: $P(1)$ est vrai, car $1 = \frac{1(1+1)}{2}$. (Le côté gauche de cette équation est 1 car 1 est la somme du premier entier positif. Le côté droit se trouve en remplaçant 1 pour n dans $n(n+1)/2$.)

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $P(k)$ vaut pour un arbitraire entier positif k . Autrement dit, nous supposons que

Si vous êtes rouillé simplifier l'algèbre expressions, c'est la le temps d'en faire révision!

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Dans cette hypothèse, il faut montrer que $P(k+1)$ est vrai, à savoir que

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}$$

est également vrai. Lorsque nous ajoutons $k + 1$ aux deux côtés de l'équation dans $P(k)$, nous obtenons

$k(k+1)$

$$
\begin{aligned}
1+2+\cdots+k+(k+1) &\overset{\text{IH}}{=} \frac{\quad}{2} + (k+1) \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}.
\end{aligned}
$$

Cette dernière équation montre que $P(k+1)$ est vrai sous l'hypothèse que $P(k)$ est vrai. Cette termine l'étape inductive.

Nous avons terminé l'étape de base et l'étape inductive, donc par induction mathématique nous sachez que $P(n)$ est vrai pour tous les entiers positifs n . Autrement dit, nous avons prouvé que $1+2+\cdots+n = n(n+1)/2$ pour tous les entiers positifs n . ▲

Comme nous l'avons noté, l'induction mathématique n'est pas un outil pour trouver des théorèmes sur tous les positifs entiers. Il s'agit plutôt d'une méthode de preuve pour prouver de tels résultats une fois qu'ils sont conjecturés. Dans Exemple 2, en utilisant l'induction mathématique pour prouver une formule de sommation, nous formulerons tous les deux puis prouver une conjecture.

EXEMPLE 2 Conjecture une formule pour la somme des n premiers entiers impairs positifs. Alors prouve ta conjecture en utilisant l'induction mathématique.

Solution: Les sommes des n premiers entiers impairs positifs pour $n = 1, 2, 3, 4, 5$ sont

$$1 = 1, \qquad 1+3 = 4, \qquad 1+3+5 = 9,$$
$$1+3+5+7 = 16, \quad 1+3+5+7+9 = 25.$$

À partir de ces valeurs, il est raisonnable de supposer que la somme des n premiers entiers impairs positifs est n^2, c'est-à-dire $1+3+5+\cdots+(2n-1) = n^2$. Nous avons besoin d'une méthode pour *prouver* que cette *conjecture* est correct, si en fait il l'est.

Soit $P(n)$ la proposition que la somme des n premiers entiers positifs impairs soit n^2. Notre la conjecture est que $P(n)$ est vrai pour tous les entiers positifs. Utiliser l'induction mathématique pour prouver cette conjecture, nous devons d'abord terminer l'étape de base; c'est-à-dire que nous devons montrer que $P(1)$ est vrai. Ensuite, nous devons effectuer l'étape inductive; c'est-à-dire que nous devons montrer que $P(k+1)$ est vrai lorsque $P(k)$ est supposé être vrai. Nous essayons maintenant de terminer ces deux étapes.

ÉTAPE DE BASE: $P(1)$ indique que la somme du premier entier positif impair est 1^2. C'est vrai car la somme du premier entier positif impair est 1. L'étape de base est terminée.

ÉTAPE INDUCTIVE: Pour terminer l'étape inductive, nous devons montrer que la proposition $P(k) \to P(k+1)$ est vrai pour chaque entier positif k . Pour ce faire, nous supposons d'abord l'inductif hypothèse. L'hypothèse inductive est la déclaration que $P(k)$ est vrai pour un positif arbitraire entier k , c'est-à-dire

$$1+3+5+\cdots+(2k-1) = k^2.$$

(Notez que le k ème entier positif impair est $(2k-1)$, car cet entier est obtenu en ajoutant 2 a total de $k-1$ fois à 1.) Pour montrer que $\forall k\,(P(k) \to P(k+1))$ est vrai, nous devons montrer que si $P(k)$ est vrai (l'hypothèse inductive), alors $P(k+1)$ est vrai. Notez que $P(k+1)$ est la déclaration que

$$1+3+5+\cdots+(2k-1)+(2k+1) = (k+1)^2.$$

Donc, en supposant que $P(k)$ est vrai, il s'ensuit que

$$
\begin{aligned}
1+3+5+\cdots+(2k-1)+(2k+1) &= [1+3+\cdots+(2k-1)]+(2k+1) \\
&\overset{\text{IH}}{=} k^2+(2k+1) \\
&= k^2+2k+1 \\
&= (k+1)^2.
\end{aligned}
$$

Cela montre que $P(k+1)$ découle de $P(k)$. Notez que nous avons utilisé l'hypothèse inductive $P(k)$ dans la deuxième égalité pour remplacer la somme des k premiers entiers positifs impairs par k^2 .

Nous avons maintenant terminé à la fois l'étape de base et l'étape inductive. Autrement dit, nous avons montré que $P(1)$ est vrai et l'instruction conditionnelle $P(k) \to P(k+1)$ est vraie pour tous les entiers positifs k . Par conséquent, par le principe de l'induction mathématique, nous pouvons conclure que $P(n)$ est vrai pour tous les entiers positifs n . Autrement dit, nous savons que $1+3+5+\cdots+(2n-1) = n^2$ pour tous positifs entiers n . ▲

Souvent, nous devrons montrer que $P(n)$ est vrai pour $n = b, b+1, b+2, \ldots,$ où b est un entier autre que 1. Nous pouvons utiliser l'induction mathématique pour y parvenir, tant que nous changeons l'étape de base en remplaçant $P(1)$ par $P(b)$. En d'autres termes, utiliser l'induction mathématique pour montrent que $P(n)$ est vrai pour $n = b, b + 1, b + 2, \ldots$, où b est un entier autre que 1, nous montrons que $P(b)$ est vrai à l'étape de base. Dans l'étape inductive, nous montrons que l'énoncé conditionnel $P(k) \rightarrow P(k+1)$ est vrai pour $k = b, b + 1, b + 2, \ldots$. Notez que b peut être négatif, nul ou positif. Suivant l'analogie domino que nous avons utilisée plus tôt, imaginez que nous commençons par en bas du b ème domino (l'étape de base), et comme chaque domino tombe, il abat le domino suivant (l'étape inductive). Nous laissons au lecteur le soin de montrer que cette forme d'induction est valable (voir Exercice 83).

Nous illustrons cette notion dans l'exemple 3, qui déclare qu'une formule de sommation est valide pour tous les entiers non négatifs. Dans cet exemple, nous devons prouver que $P(n)$ est vrai pour $n = 0, 1, 2, \ldots$. Ainsi, l'étape de base de l'exemple 3 montre que $P(0)$ est vrai.

EXEMPLE 3 Utiliser l'induction mathématique pour montrer que

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

pour tous les entiers non négatifs n .

Solution: Soit $P(n)$ la proposition selon laquelle $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ pour l'entier n .

ÉTAPE DE BASE: $P(0)$ est vrai car $2^0 = 1 = 2^1 - 1$. Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $P(k)$ est vrai pour un arbitraire entier non négatif k . Autrement dit, nous supposons que

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1.$$

Pour réaliser l'étape inductive en utilisant cette hypothèse, nous devons montrer que lorsque nous supposons que $P(k)$ est vrai, alors $P(k+1)$ est également vrai. Autrement dit, nous devons montrer que

$$1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

en supposant l'hypothèse inductive $P(k)$. Sous l'hypothèse de $P(k)$, nous voyons que

$$\begin{aligned} 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} &= (1 + 2 + 2^2 + \cdots + 2^k) + 2^{k+1} \\ &\overset{\text{IH}}{=} (2^{k+1} - 1) + 2^{k+1} \\ &= 2 \cdot 2^{k+1} - 1 \\ &= 2^{k+2} - 1. \end{aligned}$$

Notez que nous avons utilisé l'hypothèse inductive dans la deuxième équation de cette chaîne d'égalités pour remplacer $1 + 2 + 2^2 + \cdots + 2^k$ par $2^{k+1} - 1$. Nous avons terminé l'étape inductive.

Parce que nous avons terminé l'étape de base et l'étape inductive, par induction mathématique nous savons que $P(n)$ est vrai pour tous les entiers non négatifs n . Autrement dit, $1 + 2 + \cdots + 2^n = 2^{n+1} - 1$ pour tous les entiers non négatifs n . ▲

La formule donnée dans l'exemple 3 est un cas particulier d'un résultat général pour la somme des termes d'une progression géométrique (Théorème 1 dans la section 2.4). Nous utiliserons l'induction mathématique pour fournir une preuve alternative de cette formule.

EXEMPLE 4 **Sommes de progressions géométriques** Utiliser l'induction mathématique pour prouver cette formule pour la somme d'un nombre fini de termes d'une progression géométrique avec le terme initial a et commun rapport r :

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1} \quad \text{lorsque } r = 1,$$

où n est un entier non négatif.

Solution: Pour prouver cette formule à l'aide d'une induction mathématique, soit $P(n)$ la déclaration suivante: la somme des $n + 1$ premiers termes d'une progression géométrique dans cette formule est correcte.

ÉTAPE DE BASE: $P(0)$ est vrai, car

$$\frac{ar^{0+1} - a}{r - 1} = \frac{ar - a}{r - 1} = \frac{a(r - 1)}{r - 1} = a.$$

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(k)$ est vrai, où k est un entier non négatif arbitraire. Autrement dit, $P(k)$ est la déclaration que

$$a + ar + ar^2 + \cdots + ar^k = \frac{ar^{k+1} - a}{r - 1}.$$

Pour terminer l'étape inductive, nous devons montrer que si $P(k)$ est vrai, alors $P(k+1)$ est également vrai. À montrer que c'est le cas, nous ajoutons d'abord ar^{k+1} des deux côtés de l'égalité affirmée par $P(k)$. nous Trouve ça

$$a + ar + ar^2 + \cdots + ar^k + ar^{k+1} \overset{IH}{=} \frac{ar^{k+1} - a}{r - 1} + ar^{k+1}.$$

La réécriture du côté droit de cette équation montre que

$$\frac{ar^{k+1} - a}{r - 1} + ar^{k+1} = \frac{ar^{k+1} - a}{r - 1} + \frac{ar^{k+2} - ar^{k+1}}{r - 1}$$
$$= \frac{ar^{k+2} - a}{r - 1}.$$

La combinaison de ces deux dernières équations donne

$$a + ar + ar^2 + \cdots + ar^k + ar^{k+1} = \frac{ar^{k+2} - a}{r - 1}.$$

Cela montre que si l'hypothèse inductive $P(k)$ est vraie, alors $P(k+1)$ doit également être vraie. Cette complète l'argument inductif.

Nous avons terminé l'étape de base et l'étape inductive, donc par induction mathématique $P(n)$ est vrai pour tous les entiers non négatifs n . Cela montre que la formule pour la somme des termes d'un la série géométrique est correcte. ▲

Comme mentionné précédemment, la formule de l'exemple 3 est le cas de la formule de Exemple 4 avec $a = 1$ et $r = 2$. Le lecteur doit vérifier que la mise de ces valeurs pour *un* et r dans la formule générale donne la même formule que dans l'exemple 3.

PROUVER DES INÉGALITÉS L'induction mathématique peut être utilisée pour prouver une variété de les inégalités qui tiennent pour tous les entiers positifs supérieurs à un entier positif particulier, comme Les exemples 5 à 7 illustrent.

EXEMPLE 5 Utiliser l'induction mathématique pour prouver l'inégalité

$$n < 2^n$$

pour tous les entiers positifs n .

Solution: Soit $P(n)$ la proposition que $n < 2^n$.

ÉTAPE DE BASE: $P(1)$ est vrai, car $1 < 2^1 = 2$. Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: Nous supposons d'abord l'hypothèse inductive que $P(k)$ est vrai pour un arbitraire entier positif k . Autrement dit, l'hypothèse inductive $P(k)$ est la déclaration que $k < 2^k$. Compléter l'étape inductive, nous devons montrer que si $P(k)$ est vrai, alors $P(k+1)$, qui est l'énoncé que $k + 1 < 2^{k+1}$, est vrai. Autrement dit, nous devons montrer que si $k < 2^k$ alors $k + 1 < 2^{k+1}$. Montrer que cette déclaration conditionnelle est vraie pour l'entier positif k , nous ajoutons d'abord 1 aux deux côtés de $k < 2^k$, puis notez que $1 \leq 2^k$. Cela nous dit que

$$k + 1 \overset{\text{IH}}{<} 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}.$$

Cela montre que $P(k+1)$ est vrai, à savoir que $k + 1 < 2^{k+1}$, basé sur l'hypothèse que $P(k)$ est vrai. L'étape d'induction est terminée.

Par conséquent, parce que nous avons terminé à la fois l'étape de base et l'étape inductive, en le principe de l'induction mathématique nous avons montré que $n < 2^n$ est vrai pour tous les positifs entiers n . ▲

EXEMPLE 6 Utiliser l'induction mathématique pour prouver que $2^n < n!$ pour chaque entier n avec $n \geq 4$. (Notez que ce l'inégalité est fausse pour $n = 1, 2$ et 3.)

Solution: Soit $P(n)$ la proposition selon laquelle $2^n < n!$.

ÉTAPE DE BASE: Pour prouver l'inégalité pour $n \geq 4$, il faut que l'étape de base soit $P(4)$. Notez que $P(4)$ est vrai, car $2^4 = 16 < 24 = 4!$

ÉTAPE INDUCTIVE: Pour l'étape inductive, nous supposons que $P(k)$ est vrai pour un entier arbitraire k avec $k \geq 4$. Autrement dit, nous supposons que $2^k < k!$ pour l'entier positif k avec $k \geq 4$. Nous devons montrer que sous cette hypothèse, $P(k+1)$ est également vrai. Autrement dit, nous devons montrer que si $2^k < k!$ pour un entier positif arbitraire k où $k \geq 4$, puis $2^{k+1} < (k+1)!$. Nous avons

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k && \text{par définition d'exposant} \\ &< 2 \cdot k! && \text{par l'hypothèse inductive} \\ &< (k+1)\, k! && \text{parce que } 2 < k+1 \\ &= (k+1)! && \text{par définition de la fonction factorielle.} \end{aligned}$$

Cela montre que $P(k+1)$ est vrai lorsque $P(k)$ est vrai. Ceci termine l'étape inductive du preuve.

Nous avons terminé l'étape de base et l'étape inductive. Par induction mathématique $P(n)$ est vrai pour tous les entiers n avec $n \geq 4$. Autrement dit, nous avons prouvé que $2^n < n!$ est vrai pour tous entiers n avec $n \geq 4$. ▲

Une inégalité importante pour la somme des inverses d'un ensemble d'entiers positifs sera prouvé dans l'exemple 7.

EXEMPLE 7 **Une inégalité pour les nombres harmoniques** Les **nombres harmoniques** H_j, $j = 1, 2, 3, \ldots$, sont Défini par

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{j}.$$

Par exemple,

$$H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}.$$

Utilisez l'induction mathématique pour montrer que

$$H_{2^n} \geq 1 + \frac{n}{2},$$

chaque fois que n est un entier non négatif.

Solution: Pour réaliser la preuve, soit $P(n)$ la proposition que $H_{2^n} \geq 1 + \frac{n}{2}$.

ÉTAPE DE BASE: $P(0)$ est vrai, car $H_{2^0} = H_1 = 1 \geq 1 + \frac{0}{2}$.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(k)$ est vrai, c'est-à-dire $H_{2^k} \geq 1 + \frac{k}{2}$, où k est un entier non négatif arbitraire. Nous devons montrer que si $P(k)$ est vrai, puis $P(k+1)$, qui indique que $H_{2^{k+1}} \geq 1 + \frac{k+1}{2}$, est également vrai. Donc, en supposant l'inductif hypothèse, il s'ensuit que

$$
\begin{aligned}
H_{2^{k+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k} + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{par la définition de l'harmonique nombre}\\
&= H_{2^k} + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{par la définition de } 2^k \text{ ème harmonique nombre}\\
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{par l'hypothèse inductive}\\
&\geq \left(1 + \frac{k}{2}\right) + 2^k \cdot \frac{1}{2^{k+1}} && \text{car il y a } 2^k \text{ termes chacun} \geq 1/2^{k+1}\\
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2} && \text{l'annulation d'un facteur commun de } 2^k \text{ au deuxième quadrimestre}\\
&= 1 + \frac{k+1}{2}.
\end{aligned}
$$

Cela établit l'étape inductive de la preuve.

Nous avons terminé l'étape de base et l'étape inductive. Ainsi, par induction mathématique $P(n)$ est vrai pour tous les entiers non négatifs n. Autrement dit, l'inégalité $H_{2^n} \geq 1 + \frac{n}{2}$ pour l'harmonique les nombres sont valables pour tous les entiers non négatifs n. ▲

Remarque: L'inégalité établie ici montre que la **série harmonique**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$$

est une série infinie divergente. Il s'agit d'un exemple important dans l'étude des séries infinies.

FOURNIR DES RÉSULTATS DE DIVISIBILITÉ L'induction mathématique peut être utilisée pour prouver la divisibil- résultats sur les entiers. Bien que ces résultats soient souvent plus faciles à prouver en utilisant des résultats théorie des nombres, il est instructif de voir comment prouver de tels résultats en utilisant l'induction mathématique, comme l'illustrent les exemples 8 et 9.

EXEMPLE 8 Utiliser l'induction mathématique pour prouver que $n^3 - n$ est divisible par 3 chaque fois que n est un entier positif. (Notez que ceci est la déclaration avec $p = 3$ du petit théorème de Fermat, qui est Théorème 3 de la section 4.4.)

Solution: Pour construire la preuve, notons $P(n)$ la proposition: " $n^3 - n$ est divisible par 3."

ÉTAPE DE BASE: L'énoncé $P(1)$ est vrai parce que $1^3 - 1 = 0$ est divisible par 3. Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $P(k)$ est vrai; c'est-à-dire que nous supposons que $k^3 - k$ est divisible par 3 pour un entier positif arbitraire k. Pour compléter l'inductif étape, nous devons montrer que lorsque nous supposons l'hypothèse inductive, il s'ensuit que $P(k+1)$, l'affirmation que $(k+1)^3 - (k+1)$ est divisible par 3, est également vraie. Autrement dit, nous devons montrer que $(k+1)^3 - (k+1)$ est divisible par 3. Notez que

$$
\begin{aligned}
(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\
&= (k^3 - k) + 3(k^2 + k).
\end{aligned}
$$

En utilisant l'hypothèse inductive, nous concluons que le premier terme $k^3 - k$ est divisible par 3. Le le second terme est divisible par 3 car il est 3 fois un entier. Donc, par la partie (i) du théorème 1 Section 4.1, nous savons que $(k+1)^3 - (k+1)$ est également divisible par 3. Ceci complète l'inductive étape.

Parce que nous avons terminé à la fois l'étape de base et l'étape inductive, par le principe principe d'induction mathématique, nous savons que $n^3 - n$ est divisible par 3 chaque fois que n est un entier positif. ▲

L'exemple suivant présente une preuve plus difficile par induction mathématique d'une division résultat de la flexibilité.

EXEMPLE 9 Utiliser l'induction mathématique pour prouver que $7^{n+2} + 8^{2n+1}$ est divisible par 57 pour chaque non négatif entier n.

Solution: pour construire la preuve, notons $P(n)$ la proposition: «$7^{n+2} + 8^{2n+1}$ est divisible par 57. "

ÉTAPE DE BASE: Pour terminer l'étape de base, nous devons montrer que $P(0)$ est vrai, car nous voulons pour prouver que $P(n)$ est vrai pour chaque entier non négatif. Nous voyons que $P(0)$ est vrai parce que $7^{0+2} + 8^{2 \cdot 0+1} = 7^2 + 8^1 = 57$ est divisible par 57. Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $P(k)$ est vrai pour un arbitraire entier non négatif k ; autrement dit, nous supposons que $7^{k+2} + 8^{2k+1}$ est divisible par 57. Pour compléter le étape inductive, nous devons montrer que lorsque nous supposons que l'hypothèse inductive $P(k)$ est vraie, alors $P(k+1)$, l'affirmation que $7^{(k+1)+2} + 8^{2(k+1)+1}$ est divisible par 57, est également vrai.
La partie difficile de la preuve est de voir comment utiliser l'hypothèse inductive. Pour profiter de l'hypothèse inductive, nous utilisons ces étapes:

$$
\begin{aligned}
\text{sept}^{(k+1)+2} + 8^{2(k+1)+1} &= 7^{k+3} + 8^{2k+3} \\
&= 7 \cdot 7^{k+2} + 8^2 \cdot 8^{2k+1} \\
&= 7{,}7^{k+2} + 64 \cdot 8^{2k+1} \\
&= 7(7^{k+2} + 8^{2k+1}) + 57 \cdot 8^{2k+1}.
\end{aligned}
$$

Nous pouvons maintenant utiliser l'hypothèse inductive, qui stipule que $7^{k+2} + 8^{2k+1}$ est divisible par 57. Nous utiliserons les parties (i) et (ii) du théorème 1 dans la section 4.1. Par la partie (ii) de ce théorème, et l'hypothèse inductive, nous concluons que le premier terme de cette dernière somme, $7(7^{k+2} + 8^{2k+1})$, est divisible par 57. Par la partie (ii) de ce théorème, le deuxième terme de cette somme, $57 \cdot 8^{2k+1}$, est divisible par 57. Par conséquent, par la partie (i) de ce théorème, nous concluons que $7(7^{k+2} + 8^{2k+1}) + 57 \cdot 8^{2k+1} =$ $\text{sept}^{k+3} + 8^{2k+3}$ est divisible par 57. Ceci termine l'étape inductive.

Parce que nous avons terminé à la fois l'étape de base et l'étape inductive, par le principe de induction mathématique, nous savons que $7^{n+2} + 8^{2n+1}$ est divisible par 57 pour chaque non négatif entier n. ▲

FOURNIR DES RÉSULTATS SUR LES ENSEMBLES L'induction mathématique peut être utilisée pour prouver résultats sur les ensembles. En particulier, dans l'exemple 10, nous prouvons une formule pour le nombre de sous-ensembles de un ensemble fini et dans l'exemple 11 nous établissons une identité d'ensemble.

Épisode 344

une•

X

T

X

S

X { a }
une•
T

FIGURE 3 Génération de sous-ensembles d'un ensemble avec $k + 1$ éléments. Ici $T = S \cup \{ a \}$.

EXEMPLE 10 **Le nombre de sous-ensembles d'un ensemble fini** Utilisez l'induction mathématique pour montrer que si S est un ensemble fini avec n éléments, où n est un entier non négatif, alors S a 2^n sous-ensembles. (Nous allons prouver ce résultat directement de plusieurs façons au chapitre 6.)

Solution: Soit $P(n)$ la proposition selon laquelle un ensemble avec n éléments a 2^n sous-ensembles.

ÉTAPE DE BASE: $P(0)$ est vrai, car un ensemble avec zéro éléments, l'ensemble vide, a exactement $2^0 = 1$ sous-ensemble, à savoir lui-même.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $P(k)$ est vrai pour un arbitraire entier non négatif k , c'est-à-dire que nous supposons que chaque ensemble avec k éléments a 2^k sous-ensembles. Il doit montrer que sous cette hypothèse, $P(k + 1)$, qui est la déclaration que chaque ensemble avec $k + 1$ éléments a 2^{k+1} sous-ensembles, doit également être vrai. Pour le montrer, soit T un ensemble avec $k + 1$ éléments. Ensuite, il est possible d'écrire $T = S \cup \{ a \}$, où a est l'un des éléments de T et $S = T - \{ a \}$ (et donc $| S | = k$). Les sous-ensembles de T peuvent être obtenus de la manière suivante. Pour chaque sous-ensemble X de S, il y a exactement deux sous-ensembles de T , à savoir X et $X \cup \{ a \}$. (Ceci est illustré à la figure 3.) Ceux-ci constituent tous les sous-ensembles de T et sont tous distincts. Nous utilisons maintenant l'hypothèse inductive pour conclure que S a 2^k sous-ensembles, car il a k éléments. Nous savons également qu'il existe deux sous - ensembles de T pour chaque sous - ensemble de S . Par conséquent, il y a $2 \cdot 2^k = 2^{k+1}$ sous - ensembles de T . Ceci termine l'argument inductif.

Parce que nous avons terminé l'étape de base et l'étape inductive, par induction mathématique il s'ensuit que $P(n)$ est vrai pour tous les entiers non négatifs n . Autrement dit, nous avons prouvé qu'un ensemble avec n éléments a 2^n sous-ensembles chaque fois que n est un entier non négatif. ▲

EXEMPLE 11 Utiliser l'induction mathématique pour prouver la généralisation suivante d'une des lois de De Morgan:

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$

chaque fois que $A_1 , A_2 , ..., A_n$ sont des sous-ensembles d'un ensemble universel U et $n \geq 2$.

Solution: Soit $P(n)$ l'identité des n ensembles.

ÉTAPE DE BASE: La déclaration $P(2)$ affirme que $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$. C'est l'une des lois; cela a été prouvé dans l'exemple 11 de la section 2.2.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(k)$ est vrai, où k est un entier arbitraire avec $k \geq 2$; c'est-à-dire que c'est la déclaration

$$\overline{\bigcap_{j=1}^{k} A_j} = \bigcup_{j=1}^{k} \overline{A_j}$$

chaque fois que $A_1 , A_2 , ..., A_k$ sont des sous - ensembles de l'ensemble universel U . Pour effectuer l'étape inductive, nous devons montrer que cette hypothèse implique que $P(k + 1)$ est vrai. Autrement dit, nous devons montrer que si cette égalité est valable pour chaque collection de k sous-ensembles de U , elle doit également collection de $k + 1$ sous-ensembles d' U . Supposons que $A_1 , A_2 , ..., A_k , A_{k+1}$ sont des sous - ensembles de U . Quand l'hypothèse inductive est supposée tenir, il s'ensuit que

$$\overline{\bigcap_{j=1}^{k+1} A_j} = \overline{\left(\bigcap_{j=1}^{k} A_j\right) \cap A_{k+1}} \quad \text{par la définition de l'intersection}$$

$$= \overline{\left(\bigcap_{j=1}^{k} A_j\right)} \cup \overline{A_{k+1}} \quad \text{par la loi de De Morgan (où les deux ensembles sont } \bigcap_{j=1}^{k} A_j \text{ et } A_{k+1})$$

$$= \left(\bigcup_{j=1}^{k} \overline{A_j}\right) \cup \overline{A_{k+1}} \quad \text{par l'hypothèse inductive}$$

$$\bigcup^{k+1}$$

$$= \bigcup_{j=1} A_j \quad \text{par la définition de l'union.}$$

Ceci termine l'étape inductive.

Parce que nous avons terminé à la fois l'étape de base et l'étape inductive, par mathématiques induction, nous savons que $P(n)$ est vrai chaque fois que n est un entier positif, $n \geq 2$. Autrement dit, nous savons cette

$$\overline{\bigcap_{j=1}^{n} A_j} = \bigcup_{j=1}^{n} \overline{A_j}$$

chaque fois que $A_1, A_2, \ldots, A_n$ sont des sous-ensembles d'un ensemble universel U et $n \geq 2$. ▲

FOURNIR DES RÉSULTATS SUR LES ALGORITHMES Ensuite, nous donnons un exemple (quelque peu plus difficile que les exemples précédents) qui illustre l'une des nombreuses façons dont l'induction mathématique est utilisé dans l'étude des algorithmes. Nous allons montrer comment l'induction mathématique peut être utilisée pour prouver qu'un algorithme gourmand que nous avons introduit dans la section 3.1 fournit toujours une solution optimale.

EXEMPLE 12 Rappeler l'algorithme de planification des discussions discuté dans l'exemple 7 de la section 3.1. L'entrée à cet algorithme est un groupe de m discussions proposées avec des heures de début et de fin prédéfinies. Le but est pour programmer autant de ces conférences que possible dans la salle de conférence principale afin qu'il n'y ait pas deux conférences chevauchement. Supposons que la conversation t_j commence à l'instant s_j et se termine à l'instant e_j. (Deux conférences ne peuvent pas continuer dans la salle de conférence principale en même temps, mais une conférence dans cette salle peut commencer en même temps un autre se termine.)

Sans perte de généralité, nous supposons que les pourparlers sont classés par ordre non décroissant heure de fin, de sorte que $e_1 \leq e_2 \leq \cdots \leq e_m$. L'algorithme gourmand procède en sélectionnant à chaque organiser une conversation avec l'heure de fin la plus précoce parmi toutes ces discussions qui commencent au plus tôt lorsque

la dernière conférence prévue dans la salle de conférence principale est terminée. Notez qu'un entretien avec la fin la plus précoce l'heure est toujours sélectionnée en premier par l'algorithme. Nous montrerons que cet algorithme gourmand est optimal en ce sens qu'il programme toujours le plus de conférences possible dans la salle de conférence principale. Prouver l'optimalité de cet algorithme, nous utilisons l'induction mathématique sur la variable n, le nombre des entretiens programmés par l'algorithme. On laisse $P(n)$ la proposition que si l'algorithme gourmand programme n entretiens dans la salle de conférence principale, il n'est alors pas possible de programmer plus de n entretiens dans cette salle.

ÉTAPE DE BASE: Supposons que l'algorithme gourmand a réussi à planifier une seule conversation, t_1, dans la salle de conférence principale. Cela signifie qu'aucune autre conversation ne peut commencer à ou après e_1, l'heure de fin de t_1. Sinon, le premier discours de ce genre auquel nous arrivons au fur et à mesure que nous traversons les pourparlers sans ordre décroissant des heures de fin pourraient être ajoutées. Par conséquent, au temps e_1, chacune des discussions restantes doit utiliser le principal salle de conférence parce qu'ils commencent tous avant e_1 et se terminent après e_1. Il s'ensuit que deux pourparlers ne peuvent être planifié parce que les deux doivent utiliser la salle de conférence principale au temps e_1. Cela montre que $P(1)$ est true et termine l'étape de base.

ÉTAPE INDUCTIVE: L'hypothèse inductive est que $P(k)$ est vrai, où k est un arbitraire entier positif, c'est-à-dire que l'algorithme gourmand planifie toujours le plus de conversations possibles quand il sélectionne k pourparlers, où k est un entier positif, étant donné tout ensemble de pourparlers, peu importe comment beaucoup. Nous devons montrer que $P(k+1)$ découle de l'hypothèse que $P(k)$ est vraie, c'est-à-dire que nous doit montrer que sous l'hypothèse de $P(k)$, l'algorithme gourmand planifie toujours le plus pourparlers possibles quand il sélectionne $k+1$ pourparlers.

Supposons maintenant que l'algorithme gourmand ait sélectionné $k+1$ conversations. Notre première étape pour terminer l'étape inductive consiste à montrer qu'il existe un calendrier comprenant le plus de discussions possible qui contient talk t_1, une conversation avec l'heure de fin la plus rapprochée. C'est facile à voir car un calendrier qui commence par la conversation t_i dans la liste, où $i > 1$, peut être modifiée de sorte que la conversation t_1 remplace la conversation t_i. Pour voir cela, notez que parce que $e_1 \leq e_i$, toutes les conversations qui devaient suivre la conversation t_i peuvent toujours être programmées.

Une fois que nous avons inclus talk t_1, planifier les discussions de sorte que le plus grand nombre possible soit programmé est réduit à programmer autant de conversations que possible qui commencent à ou après l'heure e_1. Donc, si nous avoir programmé autant de conférences que possible, le calendrier des conférences autres que la conférence t_1 est un calendrier des discussions originales qui commencent une fois la conversation t_1 terminée. Parce que l'algorithme gourmand horaires k parle quand il crée cet horaire, on peut appliquer l'hypothèse inductive pour conclure qu'il a prévu le plus de pourparlers possible. Il s'ensuit que l'algorithme gourmand a prévu les pourparlers le plus possible, $k+1$, quand il a produit un calendrier avec $k+1$ pourparlers, donc $P(k+1)$ est vrai. Ceci termine l'étape inductive.

Nous avons terminé l'étape de base et l'étape inductive. Ainsi, par induction mathématique, nous sachez que $P(n)$ est vrai pour tous les entiers positifs n. Ceci complète la preuve de l'optimalité. C'est, nous avons prouvé que lorsque l'algorithme gourmand planifie n entretiens, lorsque n est un entier positif, il n'est alors pas possible de programmer plus de n entretiens. ▲

UTILISATIONS CRÉATIVES DE L' **INDUCTION MATHÉMATIQUE L'** induction mathématique peut souvent être utilisé de manière inattendue. Nous allons illustrer deux utilisations particulièrement intelligentes des mathématiques induction ici, le premier concernant les survivants dans un combat à tarte et le second concernant les pavages avec triominos réguliers de damiers avec un carré manquant.

EXEMPLE 13 **Combats** impairs avec des **tartes** Un nombre impair de personnes se tiennent dans une cour à des distances mutuellement distinctes. En même temps, chaque personne jette une tarte sur son voisin le plus proche, frappant cette personne. Utilisation induction mathématique pour montrer qu'il y a au moins un survivant, c'est-à-dire au moins une personne qui n'est pas touché par une tarte. (Ce problème a été introduit par Carmony [Ca79]. Notez que ce résultat est faux quand il y a un nombre pair de personnes; voir l'exercice 75.)

Solution: Soit $P(n)$ la déclaration qu'il y a un survivant chaque fois que $2n + 1$ personnes se tiennent une cour à des distances mutuelles distinctes et chaque personne jette une tarte sur son voisin le plus proche. À pour prouver ce résultat, nous montrerons que $P(n)$ est vrai pour tous les entiers positifs n. Cela suit parce que lorsque n parcourt tous les entiers positifs, $2n + 1$ parcourt tous les entiers impairs supérieurs ou égaux

à 3. Notez qu'une personne ne peut pas participer à un combat de tarte parce qu'il n'y a personne d'autre pour lancer le tarte à.

ÉTAPE DE BASE: Lorsque $n = 1$, il y a $2n + 1 = 3$ personnes dans le combat circulaire. Des trois personnes, supposons que la paire la plus proche soit A et B, et C est la troisième personne. Parce que les distances entre paires de personnes sont différentes, la distance entre A et C et la distance entre B et C sont à la fois différent et supérieur à la distance entre A et B. Il s'ensuit que A et B lancent tentes les uns aux autres, tandis que C jette une tarte à A ou B, selon ce qui est le plus proche. Par conséquent, C n'est pas touché par une tarte. Cela montre qu'au moins une des trois personnes n'est pas touchée par une tarte, complétant ainsi l'étape de base.

ÉTAPE INDUCTIVE: Pour l'étape inductive, supposons que $P(k)$ est vrai pour un impair arbitraire entier k avec $k \geq 3$. Autrement dit, supposons qu'il y ait au moins un survivant chaque fois que $2k + 1$ personnes se tenir dans une cour à des distances mutuelles distinctes et chacun lance une tarte à son voisin le plus proche. nous doit montrer que si l'hypothèse inductive $P(k)$ est vraie, alors $P(k + 1)$, l'affirmation qu'il y a au moins un survivant chaque fois que $2(k + 1) + 1 = 2k + 3$ personnes se tiennent dans une cour à une mutuelle distincte distances et chacun jette une tarte à leur plus proche voisin, est également vrai.

Supposons donc que nous ayons $2(k + 1) + 1 = 2k + 3$ personnes dans une cour avec des distances distinctes entre des paires de personnes. Soit A et B la paire de personnes la plus proche de ce groupe de $2k + 3$ personnes. Lorsque chaque personne lance une tarte à la personne la plus proche, A et B *se* lancent des tartes. Nous avons deux cas à considérer, *(i)* lorsque quelqu'un d'autre lance une tarte sur A ou B et *(ii)* lorsque personne d' autre jette une tarte aux deux A ou B.

Cas (i): Parce que A et B *se* lancent des tartes et que quelqu'un d'autre lance une tarte sur A et B, au moins trois tartes sont lancées en A et B, et au plus $(2k + 3) - 3 = 2k$ tartes sont lancées aux $2k + 1$ personnes restantes. Cela garantit qu'au moins une personne est une survivante, car si de ces $2k + 1$ personnes ont été touchées par au moins une tarte, un total d'au moins $2k + 1$ tartes devrait être jetés sur eux. (Le raisonnement utilisé dans cette dernière étape est un exemple du principe du pigeonnier discuté plus en détail à la section 6.2.)

Cas (ii): Personne d'autre jette une tarte aux deux A et B. Outre A et B, il y a $2k + 1$ personnes. Parce que les distances entre les paires de ces personnes sont toutes différentes, nous pouvons utiliser l'inductif hypothèse pour conclure qu'il y a au moins un survivant S lorsque ces $2k + 1$ personnes chacune jette une tarte à leur voisin le plus proche. De plus, S n'est pas non plus touché par la tarte lancée par A ou la tarte lancée par B parce que A et B *se* jettent leurs tartes, donc S est un survivant parce que S n'est touché par aucun des tartes lancés par ces $2k + 3$ personnes.

Nous avons terminé à la fois l'étape de base et l'étape inductive, en utilisant une preuve par cas Donc par induction mathématique, il s'ensuit que $P(n)$ est vrai pour tous les entiers positifs n. Nous concluons que chaque fois qu'un nombre impair de personnes situées dans une cour à des distances mutuelles distinctes jette chacune un tarte à leur voisin le plus proche, il y a au moins un survivant. ▲

Dans la section 1.8, nous avons discuté du carrelage des damiers par les polyominos. Exemple 14 illus- explique comment l'induction mathématique peut être utilisée pour prouver un résultat sur la couverture des damiers avec triominos droits, pièces en forme de lettre «L.»

EXEMPLE 14 Soit n un entier positif. Montrez que tous les $2^n \times 2^n$ damier avec un carré retiré peut être carrelé en utilisant des triominos droits, où ces pièces couvrent trois carrés à la fois, comme indiqué dans Figure 4.

Solution: Soit $P(n)$ la proposition selon laquelle tous les $2^n \times 2^n$ damier avec un carré retiré peut être carrelé en utilisant des triominos droits. Nous pouvons utiliser l'induction mathématique pour prouver que $P(n)$ est vrai pour tous les entiers positifs n.

FIGURE 4 **A Triomino droit.**

ÉTAPE DE BASE: $P(1)$ est vrai, car chacun des quatre damiers 2×2 avec un carré retiré peut être carrelé en utilisant un triomino droit, comme le montre la figure 5.

FIGURE 5 Carrelage 2 × 2 damiers avec un carré retiré.

ÉTAPE INDUCTIVE: L'hypothèse inductive est l'hypothèse que *P (k)* est vrai pour le positif entier k ; c'est-à-dire que c'est l'hypothèse que tous les $2^k \times 2^k$ damier avec un carré retiré peut être carrelé en utilisant des triominos droits. Il doit être démontré que dans l'hypothèse de l'induction l'hypothèse, *P (k* + 1 *)* doit également être vraie; c'est-à-dire n'importe quel $2^{k+1} \times 2^{k+1}$ damier avec un carré retiré peut être carrelé en utilisant des triominos droits.

Pour voir cela, considérez un $2^{k+1} \times 2^{k+1}$ damier avec un carré retiré. Fractionner cela damier en quatre damiers de taille $2^k \times 2^k$, en le divisant en deux dans les deux sens. Ceci est illustré à la figure 6. Aucun carré n'a été retiré de trois de ces quatre vérificateurs. planches. Le quatrième $2^k \times 2^k$ le damier a un carré retiré, donc nous utilisons maintenant l'inductif hypothèse pour conclure qu'il peut être recouvert de triominos droits. Maintenant, supprimez temporairement le carré de chacun des trois autres $2^k \times 2^k$ damiers qui a le centre de l'original, plus grand damier comme l'un de ses coins, comme le montre la figure 7. Par l'hypothèse inductive, chacun de ces trois $2^k \times 2^k$ damiers avec un carré enlevé peuvent être carrelés par trio droit non. De plus, les trois carrés qui ont été temporairement supprimés peuvent être couverts par un droit triomino. Par conséquent, l'ensemble $2^{k+1} \times 2^{k+1}$ le damier peut être carrelé avec des triominos droits.

Nous avons terminé l'étape de base et l'étape inductive. Par conséquent, par mathématique l'induction cal *P (n)* est vraie pour tous les entiers positifs n . Cela montre que nous pouvons $2^n \times 2^n$ damier, où n est un entier positif, avec un carré supprimé, en utilisant la droite triominos. ▲

FIGURE 6 Division d'un $2^{k+1} \times 2^{k+1}$ Damier en Quatre $2^k \times 2^k$ Damiers.

FIGURE 7 Mosaïque du $2^{k+1} \times 2^{k+1}$ Damier avec un carré supprimé.

Preuves erronées par induction mathématique

Consulter *les erreurs courantes en mathématiques discrètes* sur le site Web de ce livre pour des erreurs plus basiques.

Comme pour toute méthode de preuve, il existe de nombreuses possibilités d'erreurs lors de l'utilisation de induction matique. De nombreuses preuves erronées et souvent divertissantes bien connues de l'induction de déclarations manifestement fausses a été conçue, comme le montrent l'exemple 15 et Exercices 49-51. Souvent, il n'est pas facile de trouver où l'erreur de raisonnement se produit dans pris des preuves.

Pour découvrir des erreurs dans les preuves par induction mathématique, rappelez-vous que dans chaque preuve, l'étape de base et l'étape inductive doivent être effectuées correctement. Ne pas terminer l'étape de base dans une preuve supposée par induction mathématique peut conduire à des preuves erronées de clairement ridicule telles que « $n = n + 1$ chaque fois que n est un entier positif». (Nous laissons au lecteur le soin de montrent qu'il est facile de construire une étape inductive correcte dans une tentative de preuve de cette affirmation.) La localisation de l'erreur dans une preuve défectueuse par induction mathématique, comme l'illustre l'exemple 15, peut être assez délicat, surtout lorsque l'erreur est masquée dans l'étape de base.

EXEMPLE 15 Trouver l'erreur dans cette «preuve» de l'affirmation clairement fausse selon laquelle chaque ensemble de lignes dans l'avion, non dont deux parallèles se rencontrent en un point commun.

"Preuve:" Soit $P(n)$ la déclaration que chaque ensemble de n lignes dans le plan, dont deux ne sont pas parallèle, se rencontrent en un point commun. Nous allons essayer de prouver que $P(n)$ est vrai pour tout positif entiers $n \geq 2$.

ÉTAPE DE BASE: L'énoncé $P(2)$ est vrai parce que deux lignes du plan non parallèles se rencontrent en un point commun (par la définition de lignes parallèles).

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(k)$ est vrai pour le positif entier k, c'est-à-dire que l'on suppose que chaque ensemble de k lignes dans le plan, dont deux ne sont pas parallèle, se rencontrent en un point commun. Pour terminer l'étape inductive, nous devons montrer que si $P(k)$ est vrai, alors $P(k + 1)$ doit également être vrai. Autrement dit, nous devons montrer que si chaque ensemble de k lignes dans le plan, dont deux ne sont pas parallèles, se rencontrent en un point commun, puis chaque ensemble de $k + 1$ lignes dans le plan, dont deux ne sont pas parallèles, se rencontrent en un point commun. Donc, considérons un ensemble de $k + 1$ distinct lignes dans l'avion. Par l'hypothèse inductive, les k premiers de ces lignes se rencontrent en un point commun p_1. De plus, par l'hypothèse inductive, les k derniers de ces droites se rencontrent en un point commun p_2.

Nous montrerons que p_1 et p_2 doivent être le même point. Si p_1 et p_2 étaient des points différents, tous les lignes contenant les deux doivent être la même ligne car deux points déterminent une ligne. Cette contredit notre hypothèse selon laquelle toutes ces lignes sont distinctes. Ainsi, p_1 et p_2 sont le même point. Nous concluons que le point $p_1 = p_2$ se situe sur toutes les $k + 1$ droites. Nous avons montré que $P(k + 1)$ est vrai en supposant que $P(k)$ est vrai. Autrement dit, nous avons montré que si nous supposons que chaque k, $k \geq 2$, des lignes distinctes se rencontrent en un point commun, puis toutes les $k + 1$ lignes distinctes se rencontrent en un point commun. Ceci termine l'étape inductive.

Nous avons terminé l'étape de base et l'étape inductive, et soi-disant nous avons une bonne preuve par induction mathématique.

Solution: en examinant cette supposée preuve par induction mathématique, il apparaît que tout est en ordre. Cependant, il y a une erreur, comme il doit y en avoir. L'erreur est assez subtile. Soigneusement regarder l'étape inductive montre que cette étape nécessite que $k \geq 3$. Nous ne pouvons pas montrer que $P(2)$ implique $P(3)$. Lorsque $k = 2$, notre objectif est de montrer que toutes les trois lignes distinctes se rencontrent point. Les deux premières lignes doivent se rencontrer en un point commun p_1 et les deux dernières lignes doivent se rencontrer en un point commun p_2. Mais dans ce cas, p_1 et p_2 ne doivent pas nécessairement être les mêmes, car la deuxième ligne est commune aux deux ensembles de lignes. C'est là que l'étape inductive échoue. ▲

Lignes directrices pour les épreuves par induction mathématique

Les exemples 1 à 14 illustrent les preuves par induction mathématique d'un ensemble diversifié de théorèmes. Chacun de ces exemples comprend tous les éléments nécessaires à une preuve par induction mathématique. Nous avons fourni un exemple de preuve invalide par induction mathématique. Résumant quoi nous avons appris de ces exemples, nous pouvons fournir des lignes directrices utiles pour la construction preuves correctes par induction mathématique. Nous présentons maintenant ces lignes directrices.

Modèle de preuves par induction mathématique

1. Exprimez l'énoncé qui doit être prouvé sous la forme «pour tout $n \geq b$, $P(n)$ » pour un entier b.
2. Écrivez les mots «Étape de base». Montrez ensuite que $P(b)$ est vrai, en veillant à ce que la valeur de b est utilisée. Ceci termine la première partie de la preuve.
3. Écrivez les mots «Étape inductive».
4. Énoncez et identifiez clairement l'hypothèse inductive sous la forme «supposez que $P(k)$ est vrai pour un entier fixe arbitraire $k \geq b$. "
5. Énoncez ce qui doit être prouvé en supposant que l'hypothèse inductive est vraie. Autrement dit, écrivez ce que $P(k+1)$ dit.
6. Démontrez l'énoncé $P(k+1)$ en utilisant l'hypothèse $P(k)$. Assurez-vous que votre preuve est valable pour tous les entiers k avec $k \geq b$, en veillant à ce que la preuve fonctionne pour les petites valeurs de k, y compris $k = b$.
7. Identifier clairement la conclusion de l'étape inductive, par exemple en disant «ceci termine l'étape inductive. "
8. Après avoir terminé l'étape de base et l'étape inductive, énoncez la conclusion, à savoir que par induction mathématique, $P(n)$ est vrai pour tous les entiers n avec $n \geq b$.

Il vaut la peine de revoir chacune des preuves mathématiques d'induction dans les exemples 1 à 14 pour voir comment ces étapes sont terminées. Il sera utile de suivre ces lignes directrices dans les solutions du des exercices qui demandent des preuves par induction mathématique. Les lignes directrices que nous avons présentées peuvent être adapté pour chacune des variantes d'induction mathématique que nous introduisons dans les exercices et plus loin dans ce chapitre.

Des exercices

1. Il y a une infinité de gares sur un itinéraire ferroviaire. Soupperpose que le train s'arrête à la première gare et suppose que si le train s'arrête dans une gare, il s'arrête à la suivante station. Montrez que le train s'arrête dans toutes les gares.

2. Supposons que vous sachiez qu'un golfeur joue le premier trou de un parcours de golf avec un nombre infini de trous et que si ce golfeur joue un trou, puis le golfeur continue à jouer le trou suivant. Prouver que ce golfeur joue tous les trous le cours.

Utilisez l'induction mathématique dans les exercices 3 à 17 pour prouver formules d'information. Assurez-vous d'identifier où vous utilisez hypothèse ductive.

3. Soit $P(n)$ l'énoncé que $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ pour l'entier positif n.

a) Qu'est-ce que l'énoncé $P(1)$?

b) Montrer que $P(1)$ est vrai, en complétant l'étape de base de la preuve.

c) Quelle est l'hypothèse inductive?

d) Que devez-vous prouver dans l'étape inductive?

e) Terminez l'étape inductive en identifiant où vous utiliser l'hypothèse inductive.

f) Expliquez pourquoi ces étapes montrent que cette formule est vraie chaque fois que n est un entier positif.

4. Soit $P(n)$ l'énoncé selon lequel $1^3 + 2^3 + \cdots + n^3 = (n(n+1)/2)^2$ pour l'entier positif n.

a) Qu'est-ce que l'énoncé $P(1)$?

b) Montrer que $P(1)$ est vrai, en complétant l'étape de base de la preuve.

c) Quelle est l'hypothèse inductive?

d) Que devez-vous prouver dans l'étape inductive?

e) Terminez l'étape inductive en identifiant où vous utiliser l'hypothèse inductive.

f) Expliquez pourquoi ces étapes montrent que cette formule est vraie chaque fois que n est un entier positif.

5. Montrer que $1^2 + 3^2 + 5^2 + \cdots + (2n+1)^2 = (n+1)(2n+1)(2n+3)/3$ chaque fois que n est un entier non négatif.

6. Prouvez que $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ chaque fois que n est un entier positif.

7. Montrer que $3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = 3(5^{n+1} - 1)/4$ chaque fois que n est un entier non négatif.

8. Montrer que $2 - 2 \cdot 7 + 2 \cdot 7^2 - \cdots + 2(-7)^n = (1 - (-7)^{n+1})/4$ chaque fois que n est un entier non négatif.

9. a) Trouvez une formule pour la somme des n premiers même positifs entiers.

b) Prouve la formule que tu as conjecturée dans la partie (a).

10. a) Trouvez une formule pour

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}$$

en examinant les valeurs de cette expression pour les petits valeurs de n.

b) Prouve la formule que tu as conjecturée dans la partie (a).

11. a) Trouvez une formule pour

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}$$

en examinant les valeurs de cette expression pour les petits valeurs de n.

b) Prouve la formule que tu as conjecturée dans la partie (a).

12. Prouvez que

$$\sum_{j=0}^{n}\left(-\frac{1}{2}\right)^{j}=\frac{2^{n+1}+(-1)^{n}}{3\cdot 2^{n}}$$

chaque fois que n est un entier non négatif.

13. Montrer que $1^2-2^2+3^2-\cdots+(-1)^{n-1}n^2=(-1)^{n-1}n(n+1)/2$ chaque fois que n est un entier positif.

14. Démontrez que pour tout entier positif n, $\sum_{k=1}^{n}k2^{k}=(n-1)2^{n+1}+2$.

15. Montrer que pour tout entier positif n,

$$1\cdot 2+2\cdot 3+\cdots+n(n+1)=n(n+1)(n+2)/3.$$

16. Démontrez que pour tout entier positif n,

$$1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+n(n+1)(n+2)$$
$$=n(n+1)(n+2)(n+3)/4.$$

17. Prouvez que $\sum_{j=1}^{n}j^4=n(n+1)(2n+1)(3n^2+3n-1)/30$ chaque fois que n est un entier positif.

Utiliser l'induction mathématique pour prouver les inégalités dans Exercises 18-30.

18. Soit $P(n)$ l'énoncé que $n!<n^n$, où n est un entier supérieur à 1.

a) Qu'est-ce que l'énoncé $P(2)$?

b) Montrer que $P(2)$ est vrai, en complétant l'étape de base de la preuve.

c) Quelle est l'hypothèse inductive?

d) Que devez-vous prouver dans l'étape inductive?

e) Terminez l'étape inductive.

f) Expliquez pourquoi ces étapes montrent que cette inégalité est true chaque fois que n est un entier supérieur à 1.

19. Soit $P(n)$ la déclaration selon laquelle

$$1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}<2-\frac{1}{n},$$

où n est un entier supérieur à 1.

a) Qu'est-ce que l'énoncé $P(2)$?

b) Montrer que $P(2)$ est vrai, en complétant l'étape de base de la preuve.

c) Quelle est l'hypothèse inductive?

d) Que devez-vous prouver dans l'étape inductive?

e) Terminez l'étape inductive.

f) Expliquez pourquoi ces étapes montrent que cette inégalité est true chaque fois que n est un entier supérieur à 1.

20. Prouver que $3^n<n!$ si n est un entier supérieur à 6.

21. Prouve que $2^n>n^2$ si n est un entier supérieur à 4.

22. Pour quels entiers non négatifs n est $n^2\leq n!$? Prouvez votre répondre.

23. Pour lesquels les entiers non négatifs n sont $2n+3\leq 2^n$? Prouver Ta Réponse.

24. Démontrer que $1/(2n)\leq[1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1)]/(2\cdot 4\cdot\cdots\cdot 2n)$ chaque fois que n est un entier positif.

∗ **25.** Démontrer que si $h>-1$, alors $1+nh\leq(1+h)^n$ pour tous les non entiers négatifs n. C'est ce qu'on appelle **l'inégalité de Bernoulli**.

∗ **26.** Supposons que a et b sont des nombres réels avec $0<b<a$.

Démontrer que si n est un entier positif, alors $a^n-b^n\leq na^{n-1}(a-b)$.

∗ **27.** Démontrez que pour chaque entier positif n,

$$1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}>2(\sqrt{n+1}-1).$$

28. Montrer que $n^2-7n+12$ est négatif chaque fois que n est un entier avec $n\geq 3$.

Dans les exercices 29 et 30, H_n désigne le n ème nombre harmonique.

∗ **29.** Démontrer que $H_{2^n}\leq 1+n$ chaque fois que n est un in- Teger.

∗ **30.** Prouve-le

$$H_1+H_2+\cdots+H_n=(n+1)H_n-n.$$

Utilisez l'induction mathématique dans les exercices 31 à 37 pour prouver faits de visibilité.

31. Démontrer que 2 divise n^2+n chaque fois que n est un Teger.

32. Montrer que 3 divise n^3+2n chaque fois que n est positif entier.

33. Démontrer que 5 divise n^5-n chaque fois que n est un négatif entier.

34. Démontrer que 6 divise n^3-n chaque fois que n est un négatif entier.

∗ **35.** Démontrer que n^2-1 est divisible par 8 chaque fois que n est impair entier positif.

∗ **36.** Prouver que 21 divise $4^{n+1}+5^{2n-1}$ chaque fois que n est un pos- entier itif.

∗ **37.** Démontrer que si n est un entier positif, alors 133 se divise $11^{n+1}+12^{2n-1}$.

Utilisez l'induction mathématique dans les exercices 38–46 pour prouver résultats sur les ensembles.

38. Démontrer que si $A_1, A_2, \ldots, A_n$ et $B_1, B_2, \ldots, B_n$ sont des ensembles tel que $A_j\subseteq B_j$ pour $j=1, 2, \ldots, n$, alors

$$\bigcup_{j=1}^{n}A_j\subseteq\bigcup_{j=1}^{n}B_j.$$

39. Montrer que si $A_1, A_2, \ldots, A_n$ et $B_1, B_2, \ldots, B_n$ sont des ensembles tel que $A_j\subseteq B_j$ pour $j=1, 2, \ldots, n$, alors

$$\bigcap_{j=1}^{n}A_j\subseteq\bigcap_{j=1}^{n}B_j.$$

40. Montrer que si $A_1, A_2, \ldots, A_n$ et B sont des ensembles, alors

$$(A_1\cap A_2\cap\cdots\cap A_n)\cup B$$
$$=(A_1\cup B)\cap(A_2\cup B)\cap\cdots\cap(A_n\cup B).$$

41. Montrer que si $A_1, A_2, \ldots, A_n$ et B sont des ensembles, alors

Étape inductive: Supposons que $P(k)$ est vrai, de sorte que tous les chevaux de tout ensemble de k chevaux sont de la même couleur. Considérez tous les chevaux $k+1$; numéroter ces chevaux $1, 2, 3, \ldots, k, k+1$. Maintenant, le premier k de ces chevaux tous doit avoir la même couleur, et le dernier k de ceux-ci doit ont également la même couleur. Parce que l'ensemble des premiers k chevaux et l'ensemble des k derniers chevaux se chevauchent, tous $k+1$ doit être de la même couleur. Cela montre que $P(k+1)$ est vrai et termine la preuve par induction.

50. Quel est le problème avec cette «preuve»? $\sum^{n}$
"Théorème" Pour tout entier positif n,

$$(A_1 \cup A_2 \cup \cdots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B).$$

42. Montrer que si $A_1, A_2, \ldots, A_n$ et B sont des ensembles, alors

$$(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) = (A_1 \cap A_2 \cap \cdots \cap A_n) - B.$$

43. Montrer que si $A_1, A_2, \ldots, A_n$ sont des sous-ensembles d'un universel définir U, puis

$$\overline{\bigcup_{k=1} A_k} = \bigcap_{k=1}^{n} \overline{A_k}.$$

44. Montrer que si $A_1, A_2, \ldots, A_n$ et B sont des ensembles, alors

$$(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) = (A_1 \cup A_2 \cup \cdots \cup A_n) - B.$$

45. Démontrer qu'un ensemble avec n éléments a $n(n-1)/2$ sous-ensembles contenant exactement deux éléments chaque fois que n est un entier supérieur ou égal à 2.

∗ **46.** Démontrer qu'un ensemble avec n éléments a $n(n-1)(n-2)/6$ sous-ensembles contenant exactement trois éléments chaque fois que n est un entier supérieur ou égal à 3.

Dans les exercices 47 et 48, nous considérons le problème du placement tours le long d'une route droite, de sorte que chaque bâtiment sur la la route reçoit le service cellulaire. Supposons qu'un bâtiment reçoive service cellulaire s'il se trouve à moins d'un mile d'une tour.

47. Concevoir un algorithme gourmand qui utilise le nombre minimum de tours possible pour fournir un service cellulaire aux bâtiments d situés aux positions $x_1, x_2, \ldots, x_d$ à partir du début de la route. [*Astuce:* à chaque étape, allez le plus loin possible le long du route avant d'ajouter une tour pour ne laisser aucun bâtiment sans couverture.]

∗ **48.** Utiliser l'induction mathématique pour prouver que l'algorithme que vous avez conçu dans l'exercice 47 produit une solution optimale, c'est-à-dire qu'il utilise le moins de tours possible pour fournir service cellulaire à tous les bâtiments.

Les exercices 49 à 51 présentent des preuves incorrectes en utilisant induction cal. Vous devrez identifier une erreur de raisonnement dans chaque exercice.

49. Quel est le problème avec cette "preuve" que tous les chevaux sont les même couleur?

Soit $P(n)$ la proposition que tous les chevaux d'un ensemble de n chevaux sont de la même couleur.

Étape de base: Clairement, $P(1)$ est vrai.

$\sum_{i=1}^{n} i = (n + \frac{1}{2})^2/2.$

Étape de base: La formule est vraie pour $n = 1$.

Étape inductive: supposons que $\sum_{i=1}^{n} i = (n + \frac{1}{2})^2/2$. alors $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$. Par l'inductive hypothèse, $\sum_{i=1}^{n+1} i = (n + \frac{1}{2})^2/2 + n + 1 = (n^2 + n + \frac{1}{4})/2 + n + 1 = (n^2 + 3n + \frac{9}{4})/2 = (n + \frac{3}{2})^2/2 = [(n+1) + \frac{1}{2}]^2/2$, complétant le induc- étape positive.

51. Quel est le problème avec cette «preuve»?

"Théorème" Pour tout entier positif n, si x et y sont entiers positifs avec $\max(x, y) = n$, puis $x = y$.

Étape de base: Supposons que $n = 1$. Si $\max(x, y) = 1$ et x et y sont des entiers positifs, nous avons $x = 1$ et $y = 1$.

Étape inductive: Soit k un entier positif. Suppose que chaque fois que $\max(x, y) = k$ et x et y sont des entiers positifs gers, puis $x = y$. Soit maintenant $\max(x, y) = k + 1$, où x et y sont des entiers positifs. Alors $\max(x - 1, y - 1) = k$, donc par l'hypothèse inductive, $x - 1 = y - 1$. Il s'ensuit que $x = y$, complétant l'étape inductive.

52. Supposons que m et n sont des entiers positifs avec $m > n$ et f est une fonction de $\{1, 2, \ldots, m\}$ à $\{1, 2, \ldots, n\}$. Utilisez l'induction mathématique sur la variable n pour montrer que f n'est pas un à un.

∗ **53.** Utilisez l'induction mathématique pour montrer que n personnes peuvent préparer un gâteau (où chaque personne obtient un ou plusieurs morceaux de gâteau) de sorte que le gâteau soit divisé équitablement, est, dans le sens où chaque personne pense avoir atteint moins $(1/n)$ e du gâteau. [*Astuce:* pour l'étape inductive, prendre une juste part du gâteau parmi les k premiers, demander à chacun de partager sa part en ce que cette per- fils pense sont $k + 1$ parties égales, puis ont le $(k + 1)$ st personne sélectionne une portion de chacun des k personnes ple. En montrant cela produit une division juste pour $k + 1$ personnes, supposons que personne $k + 1$ pense que personne *je* suis p_i du gâteau où $\sum_{i=1}^{k} p_i = 1$.]

54. Utiliser l'induction mathématique pour montrer que, étant donné un ensemble de $n + 1$ entiers positifs, aucun ne dépassant $2n$, il y a à au moins un entier de cet ensemble qui divise un autre entier en l'ensemble.

∗ **55.** Un chevalier sur un échiquier peut déplacer un horizon d'espace- (dans les deux sens) et deux espaces verticalement (dans dans les deux sens) ou deux espaces horizontalement (dans et un espace verticalement (dans les deux sens). Supposons que nous ayons un échiquier infini, composé

de tous les carrés (m, n) où m et n sont des nombres *entiers* non négatifs gers qui indiquent le numéro de ligne et le numéro de colonne du carré, respectivement. Utilisez l'induction mathématique pour montrer qu'un chevalier commençant à (0, 0) peut visiter chaque carré en utilisant une séquence finie de mouvements. [*Astuce:* utiliser l'induction sur la variable $s = m + n$.]

56. Supposons que

$$\mathbf{A} = \begin{bmatrix} un & 0 \\ 0 & b \end{bmatrix},$$

où a et b sont des nombres réels. Montre CA

$$\mathbf{UNE}^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}$$

pour chaque entier positif n.

57. (*Calcul requis*) Usemathematicalinductiontoprove que la dérivée de $f(x) = x^n$ est égal à nx^{n-1} n'importe quand n est un entier positif. (Pour l'étape inductive, utilisez le règle de produit pour les produits dérivés.)

58. Supposons que **A** et **B** sont des matrices carrées avec la propo- propriété $\mathbf{AB} = \mathbf{BA}$. Montrez que $\mathbf{AB}^n = \mathbf{B}^n$ **Un** pour chaque positif entier n.

59. Supposons que m est un entier positif. Utiliser des mathématiques induction pour prouver que si a et b sont des entiers avec $a \equiv b \pmod{m}$, alors $a^k \equiv b^k \pmod{m}$ chaque fois que k est un

∗ **66.** Utilisez la propriété de bon ordre pour montrer que les forme d'induction mathématique est une méthode valable pour prouver que $P(n)$ est vrai pour tous les entiers positifs n.

Étape de base: $P(1)$ et $P(2)$ sont vrais.

Étape inductive: pour chaque entier positif k, si $P(k)$ et $P(k + 1)$ sont tous les deux vrais, alors $P(k + 2)$ est vrai.

67. Montrer que si $A_1, A_2, \ldots, A_n$ sont des ensembles où $n \geq 2$, et pour toutes les paires d'entiers i et j avec $1 \leq i < j \leq n$ soit A_i est un sous-ensemble de A_j ou A_j est un sous-ensemble de A_i, alors il y a un entier i, $1 \leq i \leq n$ tel que A_i est un sous-ensemble de A_j pour tous les entiers j avec $1 \leq j \leq n$.

∗ **68.** Un invité à une fête est une **célébrité** si cette personne est connue par tous les autres invités, mais n'en connaît aucun. Il y a à plus une célébrité lors d'une fête, car s'il y en avait deux, ils se connaîtraient. Une partie particulière peut célébrité. Votre mission est de trouver la célébrité, le cas échéant existe, lors d'une fête, en ne posant qu'un seul type de question ... demander à un invité s'il connaît un deuxième invité. Ev- eryone doit répondre honnêtement à vos questions. Autrement dit, si Alice et Bob sont deux personnes à la fête, vous pouvez demander à Al- glace si elle connaît Bob; elle doit répondre correctement. Utiliser l'induction mathématique pour montrer que s'il y a n les gens à la fête, alors vous pouvez trouver la célébrité, si il y en a une, avec $3(n - 1)$ questions. [*Astuce:* demandez d'abord à question d'éliminer une personne en tant que célébrité. Ensuite, utilisez entier atif

60. Utiliser l'induction mathématique pour montrer que $\neg (p_1 \vee p_2 \vee \cdots \vee p_n)$ est équivalent à $\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n$ chaque fois que $p_1, p_2, \ldots, p_n$ sont des propositions.

∗ **61.** Montre CA

$$[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n)] \to [(p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1}) \to p_n]$$

est une tautologie chaque fois que $p_1, p_2, \ldots, p_n$ sont des propositions, où $n \geq 2$.

∗ **62.** Montrer que n lignes séparent le plan en $(n^2 + n + 2)/2$ régions si pas deux de ces lignes sont parallèles et pas trois passer par un point commun.

∗∗ **63.** Soit $a_1, a_2, \ldots, a_n$ des nombres réels positifs. L' **arith-la moyenne métrique** de ces nombres est définie par

$$A = (a_1 + a_2 + \cdots + a_n)/n,$$

et la **moyenne géométrique** de ces nombres est définie par

$$G = (a_1 a_2 \cdots a_n)^{1/n}.$$

Utilisez l' induction mathématique pour prouver que $A \geq G$.

64. Utiliser l'induction mathématique pour prouver le lemme 3 de Section 4.3, qui stipule que si p est un nombre premier et $p \mid a_1 a_2 \cdots a_n$, où a_i est un entier pour $i = 1, 2, 3, \ldots, n$, puis $p \mid a_i$ pour un entier i.

65. Montrer que si n est un entier positif, alors

$$\sum_{\{a_1, \ldots, a_k\} \subseteq \{1, 2, \ldots, n\}} \frac{1}{a_1 a_2 \cdots a_k} = n.$$

(Ici, la somme est sur tous les sous-ensembles non vides de l'ensemble de les n plus petits entiers positifs.)

l'hypothèse inductive pour identifier une célébrité potentielle. Enfin, posez deux questions supplémentaires pour déterminer si cette personne est en fait une célébrité.]

Supposons qu'il y ait n personnes dans un groupe, chacune consciente d'un scandale personne d'autre dans le groupe n'est au courant. Ces personnes communiquer par téléphone; quand deux personnes dans le groupe parlent, elles partager des informations sur tous les scandales que chacun connaît. Pour exemple, lors du premier appel, deux personnes partagent des informations, à la fin de l'appel, chacune de ces personnes connaît deux scandales. Le **problème des potins** demande $G(n)$, le minimum nombre d'appels téléphoniques nécessaires pour que toutes les n personnes en savoir plus sur tous les scandales. Les exercices 69 à 71 traitent des problème de potins.

69. Trouvez $G(1)$, $G(2)$, $G(3)$ et $G(4)$.

70. Utiliser l'induction mathématique pour prouver que $G(n) \leq 2n - 4$ pour $n \geq 4$. [*Astuce:* Dans l'étape inductive, demandez à une nouvelle personne appeler une personne en particulier au début et à la fin.]

∗∗ **71.** Démontrer que $G(n) = 2n - 4$ pour $n \geq 4$.

∗ **72.** Montrer qu'il est possible d'organiser les nombres $1, 2, \ldots, n$ d'affilée de sorte que la moyenne de deux de ces nombres n'apparaît jamais entre eux. [*Indice:* montrez que cela suffit pour prouver ce fait lorsque n est une puissance de 2. Ensuite, utilisez math-induction ématique pour prouver le résultat lorsque n est une puissance of 2.]

∗ **73.** Montrer que si $I_1, I_2, \ldots, I_n$ est une collection d'in-tervaux sur la droite du nombre réel, $n \geq 2$, et chaque paire de ces intervalles a une intersection non vide, c'est-à-dire, $I_i \cap I_j \neq \emptyset$ chaque fois que $1 \leq i \leq n$ et $1 \leq j \leq n$, alors l'intersection de tous ces ensembles est non vide, c'est-à-dire $I_1 \cap I_2 \cap \cdots \cap I_n \neq \emptyset$. (Rappelons qu'un **intervalle ouvert** est

l'ensemble des nombres réels x avec $a < x < b$, où a et b sont des nombres réels avec $a < b$.)

Parfois, nous ne pouvons pas utiliser l'induction mathématique pour prouver un résultat que nous croyons être vrai, mais nous pouvons utiliser des mathématiques induction pour prouver un résultat plus fort. Parce que l'hyper inductif la thèse du résultat le plus fort offre plus de travail avec, ce processus est appelé **chargement inductif**. Nous utilisons un chargement inductif dans l'exercice 74.

74. Supposons que nous voulons prouver que

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}$$

pour tous les entiers positifs n.

a) Montrez que si nous essayons de prouver cette inégalité en utilisant l'induction ématique, l'étape de base fonctionne, mais échec de l'étape ductive.

b) Montrer que l'induction mathématique peut être utilisée pour prouver l'inégalité plus forte

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}$$

pour tous les entiers supérieurs à 1, qui, avec un vérification pour le cas où $n = 1$, établit le une inégalité plus faible, nous avons initialement essayé de prouver en utilisant Induction mathematique.

75. Soit n un entier pair positif. Montrer que lorsque n personne se tiennent dans une cour à des distances mutuellement distinctes et personne jette une tarte sur son voisin le plus proche, il est possible que tout le monde est touché par une tarte.

76. Construire un carrelage en utilisant des triominos droits du 4×4 damier avec le carré dans le coin supérieur gauche déplacé.

77. Construire un carrelage en utilisant des triominos droits du 8×8 damier avec le carré dans le coin supérieur gauche déplacé.

78. Prouver ou infirmer que tous les damiers de ces formes peut être complètement recouvert en utilisant des triominos droits quand-toujours n est un entier positif.

a) 3×2^n **b)** 6×2^n
c) $3^n \times 3^n$ **d)** $6^n \times 6^n$

∗ **79.** Montrez qu'un 2 en trois dimensions $^n \times 2^n \times 2^n$ vérificateur-conseil avec un $1 \times 1 \times 1$ cube manquant peut être complètement recouvert de $2 \times 2 \times 2$ cubes avec un cube $1 \times 1 \times 1$ déplacé.

∗ **80.** Montrer qu'un damier $n \times n$ avec un carré déplacé peut être complètement recouvert en utilisant des triominos droits si $n > 5$, n est impair et $3 \mid n$.

81. Montrer qu'un damier 5×5 avec un carré d'angle déplacé peut être carrelé en utilisant des triominos droits.

∗ **82.** Trouvez un damier 5×5 avec un carré retiré qui ne peut pas être carrelé avec des triominos appropriés. Prouver qu'un tel le carrelage n'existe pas pour ce panneau.

83. Utiliser le principe de l'induction mathématique pour montrer que $P(n)$ est vrai pour $n = b, b + 1, b + 2, \ldots$, où b est un entier, si $P(b)$ est vrai et l'instruction conditionnelle $P(k) \to P(k + 1)$ est vrai pour tous les entiers k avec $k \geq b$.

Induction forte et bon ordre

introduction

Dans la section 5.1, nous avons introduit l'induction mathématique et nous avons montré comment l'utiliser pour prouver variété de théorèmes. Dans cette section, nous allons introduire une autre forme d'induction mathématique, appelé **forte induction**, qui peut souvent être utilisé lorsque nous ne pouvons pas facilement prouver un résultat en utilisant

Induction mathematique. L'étape de base d'une preuve par induction forte est la même qu'une preuve de le même résultat en utilisant l'induction mathématique. Autrement dit, dans une forte preuve d'induction que $P(n)$ est vrai pour tous les entiers positifs n, l'étape de base montre que $P(1)$ est vrai. Cependant, les étapes inductives dans ces deux méthodes de preuve sont différentes. Dans une preuve par induction mathématique, l'inductif étape montre que si l'hypothèse inductive $P(k)$ est vraie, alors $P(k+1)$ est également vraie. Dans une preuve par forte induction, l'étape inductive montre que si $P(j)$ est vrai pour tous les entiers positifs non dépassant k, alors $P(k+1)$ est vrai. Autrement dit, pour l'hypothèse inductive, nous supposons que $P(j)$ est vrai pour $j = 1, 2, ..., k$.

La validité de l'induction mathématique et de l'induction forte découle de la bonne ordonner la propriété dans l'annexe 1. En fait, l'induction mathématique, l'induction forte et l'ordre est tous des principes équivalents (comme le montrent les exercices 41, 42 et 43). Autrement dit, la validité de chacun peut être prouvé par l'un ou l'autre. Cela signifie qu'une preuve utilisant l'un de ces deux principes peuvent être réécrits comme preuve en utilisant l'un ou l'autre des deux autres principes. Tout comme c'est parfois, il est beaucoup plus facile de voir comment prouver un résultat en utilisant une forte induction plutôt que l'induction mathématique, il est parfois plus facile d'utiliser le bon ordre que l'un des

deux formes d'induction mathématique. Dans cette section, nous donnerons quelques exemples de la une propriété de bon ordre peut être utilisée pour prouver des théorèmes.

Forte induction

Avant d'illustrer comment utiliser une forte induction, nous énonçons à nouveau ce principe.

INDUCTION FORTE Pour prouver que $P(n)$ est vrai pour tous les entiers positifs n, où $P(n)$ est une fonction propositionnelle, nous effectuons deux étapes:

ÉTAPE DE BASE: Nous vérifions que la proposition $P(1)$ est vraie.

ÉTAPE INDUCTIVE: Nous montrons que l'énoncé conditionnel $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ est vrai pour tous les entiers positifs k.

Notez que lorsque nous utilisons une forte induction pour prouver que $P(n)$ est vrai pour tous les entiers positifs n, notre hypothèse inductive est l'hypothèse que $P(j)$ est vraie pour $j = 1, 2, ..., k$. C'est le l'hypothèse inductive inclut toutes les k déclarations $P(1), P(2), \ldots, P(k)$. Parce que nous pouvons utiliser tous les k déclarations $P(1), P(2), \ldots, P(k)$ pour prouver $P(k+1)$, plutôt que simplement l'énoncé $P(k)$ comme dans un preuve par induction mathématique, une forte induction est une technique de preuve plus flexible. Car certains mathématiciens préfèrent toujours utiliser une forte induction au lieu de mathématiques induction, même lorsqu'une preuve par induction mathématique est facile à trouver.

Vous pourriez être surpris que l'induction mathématique et l'induction forte soient équivalentes. C'est-à-dire que chacun peut être montré comme une technique de preuve valide en supposant que l'autre est valide. Dans En particulier, toute preuve utilisant l'induction mathématique peut également être considérée comme une preuve par induction parce que l'hypothèse inductive d'une preuve par induction mathématique fait partie de la hypothèse inductive dans une preuve par forte induction. Autrement dit, si nous pouvons terminer l'inductive étape d'une preuve par induction mathématique en montrant que $P(k+1)$ découle de $P(k)$ pour chaque entier positif k, il s'ensuit également que $P(k+1)$ résulte de toutes les déclarations $P(1)$, $P(2), \ldots, P(k)$, parce que nous supposons que non seulement $P(k)$ est vrai, mais aussi plus, à savoir que les $k-1$ déclarations $P(1), P(2), \ldots, P(k-1)$ sont vrais. Cependant, il est beaucoup plus gênant de convertir une preuve par forte induction en une preuve en utilisant le principe de l'induction mathématique. (Voir l'exercice 42.)

L'induction forte est parfois appelée le **deuxième principe de l'induction mathématique** ou **induction complète**. Lorsque la terminologie «induction complète» est utilisée, le principe de l'induction mathématique est appelée **induction incomplète**, un terme technique qui est un peu choix malheureux car le principe de mathématique n'a rien d'incomplet induction; après tout, c'est une technique de preuve valable.

INDUCTION FORTE ET ÉCHELLE INFINIE Pour mieux comprendre les production, considérons l'échelle infinie de la section 5.1. Une forte induction nous dit que nous pouvons atteindre tous les échelons si

1. nous pouvons atteindre le premier échelon, et
2. pour chaque entier k, si nous pouvons atteindre tous les k premiers barreaux, alors nous pouvons atteindre le $(k+1)$ st barreau.

Autrement dit, si $P(n)$ est la déclaration selon laquelle nous pouvons atteindre le n ème échelon de l'échelle, par forte induction nous savons que $P(n)$ est vrai pour tous les entiers positifs n, car (1) nous dit que $P(1)$ est vrai, complétant l'étape de base et (2) nous dit que $P(1) \wedge P(2) \wedge \cdots \wedge P(k)$ implique $P(k+1)$, complétant la étape inductive.

L'exemple 1 illustre comment une forte induction peut nous aider à prouver un résultat qui ne peut pas être facilement prouvé en utilisant le principe de l'induction mathématique.

EXEMPLE 1 Supposons que nous puissions atteindre les premier et deuxième échelons d'une échelle infinie, et nous savons que si nous peut atteindre un échelon, alors nous pouvons atteindre deux échelons plus haut.Pouvons-nous prouver que nous pouvons atteindre barré en utilisant le principe de l'induction mathématique?Pouvons-nous prouver que nous pouvons atteindre chaque échelon en utilisant une forte induction?

Solution: Nous essayons d'abord de prouver ce résultat en utilisant le principe de l'induction mathématique.

ÉTAPE DE BASE: L'étape de base d'une telle preuve tient;ici, il vérifie simplement que nous pouvons atteindre le premier échelon.

ÉTAPE INDUCTIVE TENTÉE: L'hypothèse inductive est la déclaration que nous pouvons atteindre le k ème barreau de l'échelle. Pour terminer l'étape inductive, nous devons montrer que si nous supposons l'hypothèse inductive pour l'entier positif k , à savoir, si nous supposons que nous pouvons atteindre le k ème échelon de l'échelle, alors nous pouvons montrer que nous pouvons atteindre le $(k + 1)$ er échelon du échelle. Cependant, il n'existe aucun moyen évident de terminer cette étape inductive car nous ne savoir à partir des informations données que nous pouvons atteindre le $(k + 1)$ premier échelon à partir du k ème échelon. Après tous, nous savons seulement que si nous pouvons atteindre un échelon, nous pouvons atteindre l'échelon deux plus haut.

Considérons maintenant une preuve utilisant une forte induction.

ÉTAPE DE BASE: L'étape de base est la même que précédemment;il vérifie simplement que nous pouvons atteindre le premier échelon.

ÉTAPE INDUCTIVE: L'hypothèse inductive stipule que nous pouvons atteindre chacun des k premiers échelons. Pour terminer l'étape inductive, nous devons montrer que si nous supposons que l'hypothèse inductive est vrai, c'est-à-dire que si nous pouvons atteindre chacun des k premiers barreaux, alors nous pouvons atteindre le $(k + 1)$ premier barreau. Nous savons déjà que nous pouvons atteindre le deuxième échelon. Nous pouvons terminer l'étape inductive en notant que tant que $k \geq 2$, nous pouvons atteindre le $(k + 1)$ premier échelon à partir du $(k - 1)$ premier échelon parce que nous savons que nous pouvons monter deux échelons à partir d'un échelon que nous pouvons déjà atteindre, et parce que $k - 1 \leq k$, par l'hypothèse inductive on peut atteindre le $(k - 1)$ premier échelon. Ceci termine l'étape inductive et termine la preuve par forte induction.

Nous avons prouvé que si nous pouvons atteindre les deux premiers échelons d'une échelle infinie et pour chaque entier positif k si nous pouvons atteindre tous les k premiers échelons, alors nous pouvons atteindre le $(k + 1)$ er échelon, puis nous pouvons atteindre tous les échelons de l'échelle. ▲

Exemples de preuves utilisant une forte induction

Maintenant que nous avons à la fois une induction mathématique et une forte induction, comment décider méthode à appliquer dans une situation particulière? Bien qu'il n'y ait pas de réponse coupée et séchée, nous pouvons fournir des conseils utiles. En pratique, vous devez utiliser l'induction mathématique simple pour prouver que $P(k) \rightarrow P(k + 1)$ est vrai pour tous les entiers positifs k . C'est le cas pour toutes les preuves dans les exemples de la section 5.1.En général, vous devez limiter votre utilisation de le principe de l'induction mathématique de tels scénarios. À moins que vous ne puissiez voir clairement que étape inductive d'une preuve par induction mathématique passe, vous devez essayer une preuve par forte induction. Autrement dit, utilisez une forte induction et non une induction mathématique lorsque vous voir comment prouver que $P(k + 1)$ est vrai à partir de l'hypothèse que $P(j)$ est vrai pour tous les positifs les entiers j ne dépassant pas k , mais vous ne voyez pas comment prouver que $P(k + 1)$ découle de $P(k)$. Gardez cela à l'esprit lorsque vous examinez les preuves de cette section. Pour chacune de ces preuves, considérez pourquoi une forte induction fonctionne mieux qu'une induction mathématique.

Nous allons illustrer comment une forte induction est employée dans les exemples 2 à 4.Dans ces exemples, nous prouverons une collection diversifiée de résultats. Portez une attention particulière à l'étape inductive chacun de ces exemples, où nous montrons qu'un résultat $P(k + 1)$ suit sous l'hypothèse que $P(j)$ est valable pour tous les entiers positifs j ne dépassant pas k , où $P(n)$ est une fonction propositionnelle.

Nous commençons par l'une des utilisations les plus importantes de l'induction forte, la partie du fondamental théorème d'arithmétique qui nous dit que tout entier positif peut être écrit comme le produit de nombres premiers.

EXEMPLE 2 Montrer que si n est un entier supérieur à 1, alors n peut être écrit comme le produit de nombres premiers.

Solution: Soit $P(n)$ la proposition selon laquelle n peut être écrit comme le produit de nombres premiers.

ÉTAPE DE BASE: $P(2)$ est vrai, car 2 peut être écrit comme le produit d'un premier, lui-même.(Remarque que $P(2)$ est le premier cas que nous devons établir.)

ÉTAPE INDUCTIVE: L'hypothèse inductive est l'hypothèse que $P(j)$ est vrai pour tous entiers j avec $2 \leq j \leq k$, c'est-à-dire l'hypothèse que j peut être écrit comme le produit de nombres premiers chaque fois que j est un entier positif d'au moins 2 et ne dépassant pas k. Pour terminer l'étape inductive, il faut montrer que $P(k + 1)$ est vrai dans cette hypothèse, c'est-à-dire que $k + 1$ est le produit des nombres premiers.

Il y a deux cas à considérer, à savoir quand $k + 1$ est premier et quand $k + 1$ est composite. Si $k + 1$ est premier, on voit immédiatement que $P(k + 1)$ est vrai. Sinon, $k + 1$ est composite et peut être écrit comme le produit de deux entiers positifs a et b avec $2 \leq a \leq b < k + 1$. Parce que à la fois *un* et b sont des nombres entiers d' au moins 2 et inférieure ou égale à k, on peut utiliser l'hypothèse de récurrence de écrivez a et b comme le produit de nombres premiers. Ainsi, si $k + 1$ est composite, il peut s'écrire comme produit des nombres premiers, à savoir, ces nombres premiers dans la factorisation de a et ceux dans la factorisation de b. ▲

Remarque: Parce que 1 peut être considéré comme le produit *vide* d'aucun nombre premier, nous aurions pu commencer la preuve dans l'exemple 2 avec $P(1)$ comme étape de base. Nous avons choisi de ne pas le faire parce que beaucoup de gens trouver cela déroutant.

L'exemple 2 complète la preuve du théorème fondamental de l'arithmétique, qui affirme que chaque entier non négatif peut s'écrire uniquement comme le produit de nombres premiers en non décroissant commande. Nous avons montré à la section 4.3 qu'un entier a au plus une telle factorisation en nombres premiers. L'exemple 2 montre qu'il existe au moins une telle factorisation.

Ensuite, nous montrons comment une forte induction peut être utilisée pour prouver qu'un joueur a un gain stratégie dans un jeu.

EXEMPLE 3 Considérons un jeu dans lequel deux joueurs à tour de rôle suppriment tout nombre positif de matchs qu'ils veulent de l'un des deux tas d'allumettes. Le joueur qui supprime le dernier match remporte la partie. Montrez que si les deux piles contiennent initialement le même nombre de matchs, le deuxième joueur peut toujours garantir une victoire.

Solution: Soit n le nombre de matchs dans chaque pile. Nous utiliserons une forte induction pour prouver $P(n)$, la déclaration selon laquelle le deuxième joueur peut gagner lorsqu'il y a initialement n matchs dans chaque pile.

ÉTAPE DE BASE: Lorsque $n = 1$, le premier joueur n'a qu'un choix, retirer un match d'un des piles, laissant une seule pile avec un seul match, que le deuxième joueur peut retirer pour gagner le match.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(j)$ est vrai pour tout j avec $1 \leq j \leq k$, c'est-à-dire l'hypothèse que le deuxième joueur peut toujours gagner chaque fois qu'il y a j matchs, où $1 \leq j \leq k$ dans chacune des deux piles au début de la partie. Nous devons montrer que $P(k + 1)$ est vrai, c'est-à-dire que le deuxième joueur peut gagner lorsqu'il y a initialement $k + 1$ matchs dans chaque pile, sous l'hypothèse que $P(j)$ est vrai pour $j = 1, 2, ..., k$. Supposons donc qu'il y ait $k + 1$ matchs dans chacune des deux piles au début de la partie et supposons que le premier joueur supprime r allumettes $(1 \leq r \leq k)$ de l'une des piles, laissant $k + 1 - r$ allumettes dans cette pile. En supprimant le même nombre de matchs de l'autre pile, le deuxième joueur crée le situation où il y a deux piles chacune avec $k + 1 - r$ correspondances. Parce que $1 \leq k + 1 - r \leq k$, nous pouvons maintenant utiliser l'hypothèse inductive pour conclure que le deuxième joueur peut toujours gagner. Nous complétons la preuve en notant que si le premier joueur retire tous les $k + 1$ matchs de l'un des les piles, le deuxième joueur peut gagner en supprimant tous les matchs restants. ▲

En utilisant le principe de l'induction mathématique, au lieu de l'induction forte, pour prouver la les résultats des exemples 2 et 3 sont difficiles. Cependant, comme le montre l'exemple 4, certains résultats peuvent être facilement prouvé en utilisant soit le principe de l'induction mathématique, soit l'induction forte.

Avant de présenter l'exemple 4, notez que nous pouvons légèrement modifier l'induction forte pour gérer une plus grande variété de situations. En particulier, nous pouvons adapter une forte induction pour gérer les cas où l'étape inductive n'est valable que pour des entiers supérieurs à un entier particulier. Soit b un fixe entier et j un entier positif fixe. La forme d'induction forte dont nous avons besoin nous dit que $P(n)$ est vrai pour tous les entiers n avec $n \geq b$ si nous pouvons effectuer ces deux étapes:

ÉTAPE DE BASE: Nous vérifions que les propositions $P(b), P(b + 1), \ldots, P(b + j)$ sont vrais.

ÉTAPE INDUCTIVE: Nous montrons que $[P(b) \wedge P(b + 1) \wedge \cdots \wedge P(k)] \rightarrow P(k + 1)$ est vrai pour chaque entier $k \geq b + j$.

Nous utiliserons cette forme alternative dans la preuve d'induction forte de l'exemple 4. Que cette la forme alternative est équivalente à une forte induction est laissée comme exercice 28.

EXEMPLE 4 Prouver que chaque montant d'affranchissement de 12 cents ou plus peut être formé en utilisant seulement 4 cents et Timbres de 5 cents.

Solution: Nous prouverons ce résultat en utilisant le principe de l'induction mathématique. Ensuite, nous présenter une preuve en utilisant une forte induction. Soit $P(n)$ la déclaration selon laquelle l'affranchissement de n cents peut être formé en utilisant des timbres de 4 et 5 cents.

Nous commençons par utiliser le principe de l'induction mathématique.

*ÉTAPE DE BASE: l'*affranchissement de 12 cents peut être formé en utilisant trois timbres de 4 cents.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(k)$ est vrai. Autrement dit, sous cette hypothèse, l'affranchissement de k cents peut être formé en utilisant destimbres de 4 cents et 5 cents. Compléter l'étape inductive, nous devons montrer que lorsque nous supposons que $P(k)$ est vrai, alors $P(k + 1)$ est également vrai où $k \geq 12$. Autrement dit, nous devons montrer que si nous pouvons former un affranchissement de k cents, alors nous pouvons sous forme d'affranchissement de $k + 1$ cents. Supposons donc que l'hypothèse inductive est vraie; c'est-à-dire, supposons que nous pouvons former un affranchissement de k cents en utilisant des timbres de 4 et 5 cents. Nous considérons deux cas, au moins un timbre de 4 cents a été utilisé et lorsqu'aucun timbre de 4 cents n'a été utilisé. Supposons d'abord qu'au moins un timbre de 4 cents a été utilisé pour former un affranchissement de k cents. Ensuite, nous pouvons remplacer cela timbre avec un timbre de 5 cents pour former un affranchissement de $k + 1$ cents. Mais si aucun timbre de 4 cents n'a été utilisé, nous pouvons former un affranchissement de k cents en utilisant seulement des timbres de 5 cents. De plus, parce que $k \geq 12$, nous avions besoin au moins trois timbres de 5 cents pour former un affranchissement de k cents. Ainsi, nous pouvons remplacer trois timbres de 5 cents avec quatre timbres de 4 cents pour former un affranchissement de $k + 1$ cents. Ceci termine l'étape inductive.

Parce que nous avons terminé l'étape de base et l'étape inductive, nous savons que $P(n)$ est vrai pour tout $n \geq 12$. Autrement dit, nous pouvons former un affranchissement de n cents, où $n \geq 12$ en utilisant seulement 4 cents et Timbres de 5 cents. Ceci complète la preuve par induction mathématique.

Ensuite, nous utiliserons une forte induction pour prouver le même résultat. Dans cette preuve, dans l'étape de base nous montrons que $P(12)$, $P(13)$, $P(14)$ et $P(15)$ sont vrais, c'est-à-dire que l'affranchissement de 12, 13, 14, ou 15 cents peuvent être formés en utilisant seulement des timbres de 4 et 5 cents. Dans l'étape inductive, nous montrons comment obtenir l'affranchissement de $k + 1$ cents pour $k \geq 15$ à partir de l'affranchissement de $k - 3$ cents.

ÉTAPE DE BASE: Nous pouvons former un affranchissement de 12, 13, 14 et 15 cents en utilisant trois timbres de 4 cents, deux Timbres de 4 cents et un timbre de 5 cents, un timbre de 4 cents et deux timbres de 5 cents et trois timbres de 5 cents timbres, respectivement. Cela montre que $P(12)$, $P(13)$, $P(14)$ et $P(15)$ sont vrais. Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que $P(j)$ est vrai pour $12 \leq j \leq k$,
où k est un entier avec $k \geq 15$. Pour terminer l'étape inductive, nous supposons que nous pouvons former
affranchissement de j cents, où $12 \leq j \leq k$. Nous devons montrer que sous l'hypothèse que $P(k+1)$
c'est vrai, on peut aussi faire des frais de port de $k+1$ centimes. En utilisant l'hypothèse inductive, nous pouvons supposer
que $P(k-3)$ est vrai parce que $k-3 \geq 12$, c'est-à-dire que nous pouvons former un affranchissement de $k-3$ cents en utilisant
seulement des timbres de 4 et 5 cents. Pour former un affranchissement de $k+1$ cents, nous devons seulement ajouter un autre 4 cents
timbre aux timbres que nous avons utilisés pour former un affranchissement de $k-3$ cents. Autrement dit, nous avons montré que si le
l'hypothèse inductive est vraie, alors $P(k+1)$ est également vrai. Ceci termine l'étape inductive.

Parce que nous avons terminé l'étape de base et l'étape inductive d'une preuve d'induction forte,
nous savons par forte induction que $P(n)$ est vrai pour tous les entiers n avec $n \geq 12$. Autrement dit, nous savons
que chaque affranchissement de n cents, où n est au moins 12, peut être formé en utilisant 4 cents et 5 cents
timbres. Ceci termine la preuve par une forte induction.

(Il existe d'autres façons d'aborder ce problème en plus de celles décrites ici. Pouvez-vous trouver
une solution qui n'utilise pas l'induction mathématique?) ▲

Utilisation d'une forte induction dans la géométrie informatique

Notre prochain exemple d'induction forte proviendra de **la géométrie informatique** , la partie de
mathématiques discrètes qui étudient les problèmes de calcul impliquant des objets géométriques. Compu-
La géométrie rationnelle est largement utilisée en infographie, jeux informatiques, robotique, scientifique
calculs, et une vaste gamme d'autres domaines. Avant de pouvoir présenter ce résultat, nous introduisons
une terminologie, peut-être familière des études antérieures en géométrie.

Un **polygone** est une figure géométrique fermée constituée d'une séquence de segments de ligne
$s_1, s_2, \ldots, s_n$, appelés **côtés** . Chaque paire de côtés consécutifs, s_i et s_{i+1} , $i = 1, 2, \ldots, n-1$,
ainsi que le dernier côté s_n et le premier côté s_1 , du polygone se rencontrent en un point final commun,
appelé un **sommet** . Un polygone est appelé **simple** s'il n'y a pas deux côtés non consécutifs qui se croisent. Chaque sim-
pli polygone divise le plan en deux régions: son **intérieur** , constitué des points à l'intérieur du
courbe, et son **extérieur** , composé des points à l'extérieur de la courbe. Ce dernier fait est étonnamment
compliqué à prouver. C'est un cas particulier du célèbre théorème de la courbe de Jordan, qui nous dit
que chaque courbe simple divise le plan en deux régions; voir [Or00], par exemple.

Un polygone est appelé **convexe** si chaque segment de ligne reliant deux points à l'intérieur du
le polygone se trouve entièrement à l'intérieur du polygone. (Un polygone qui est non convexe est dite **non - convexe**).
La figure 1 montre quelques polygones; les polygones (a) et (b) sont convexes, mais les polygones (c) et (d) sont
ne pas. Une **diagonale** d'un polygone simple est un segment de ligne reliant deux sommets non consécutifs de
le polygone, et une diagonale est appelée une **diagonale intérieure** si elle se trouve entièrement à l'intérieur du polygone, ex-
cept pour ses points de terminaison. Par exemple, dans le polygone (d), le segment de ligne reliant a et f est un entier
diagonale supérieure, mais le segment de ligne reliant a et d est une diagonale qui n'est pas une diagonale intérieure.

L'une des opérations les plus élémentaires de la géométrie informatique consiste à diviser un simple
polygone en triangles en ajoutant des diagonales sans intersection. Ce processus est appelé **triangulation** .
Notez qu'un simple polygone peut avoir de nombreuses triangulations différentes, comme le montre la figure 2. Peut-être
le fait le plus fondamental de la géométrie de calcul est qu'il est possible de trianguler chaque simple

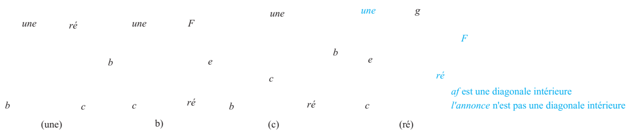


FIGURE 1 **Polygones convexes et non convexes.**

Page 360

Deux triangulations différentes d'un polygone simple avec sept côtés en cinq triangles,
montré avec des lignes pointillées et des lignes pointillées, respectivement

FIGURE 2 **Triangulations d'un polygone.**

polygone, comme nous le disons dans le théorème 1. En outre, ce théorème nous dit que chaque triangulation d'un polygone simple avec n côtés comprend n - 2 triangles.

THÉORÈME 1 Un polygone simple à n côtés, où n est un entier avec $n \geq 3$, peut être triangulé en n - 2 triangles.

Il semble évident que l'on devrait pouvoir trianguler un simple polygone en successivement ajout de diagonales intérieures. Par conséquent, une preuve par forte induction semble prometteuse. cependant, une telle preuve nécessite ce lemme crucial.

LEMMA 1 Chaque polygone simple avec au moins quatre côtés a une diagonale intérieure.

Bien que le lemme 1 semble particulièrement simple, il est étonnamment difficile à prouver. En fait, comme il y a seulement 30 ans, une variété de preuves incorrectes considérées comme correctes ont été fréquemment vues dans des livres et des articles. Nous reportons la preuve du lemme 1 jusqu'à ce que nous prouvions le théorème 1. Ce n'est pas rare de prouver un théorème en attendant la preuve ultérieure d'un lemme important.

Preuve (du théorème 1): Nous prouverons ce résultat en utilisant une forte induction. Soit $T(n)$ le énoncer que chaque polygone simple avec n côtés peut être triangulé en n - 2 triangles.

ÉTAPE DE BASE: $T(3)$ est vrai car un simple polygone à trois côtés est un triangle. On n'a pas besoin pour ajouter des diagonales pour trianguler un triangle; il est déjà triangulé en un triangle lui-même. Par conséquent, chaque polygone simple avec $n = 3$ a peut être triangulé en $n - 2 = 3 - 2 = 1$ Triangle.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $T(j)$ est vrai pour tous entiers j avec $3 \leq j \leq k$. Autrement dit, nous supposons que nous pouvons trianguler un simple polygone avec j côtés en j - 2 triangles chaque fois que $3 \leq j \leq k$. Pour terminer l'étape inductive, nous doit montrer que lorsque nous supposons l'hypothèse inductive, $P(k+1)$ est vrai, c'est-à-dire que tout un polygone simple avec k + 1 côtés peut être triangulé en $(k + 1) - 2 = k - 1$ triangles.

Supposons donc que nous ayons un simple polygone P avec k + 1 côtés. Parce que $k + 1 \geq 4$, Lemme 1 nous dit que P a une diagonale intérieure ab. Maintenant, ab divise P en deux polygones simples Q, avec côtés s, et R, avec côtés t. Les côtés de Q et R sont les côtés de P, avec le côté ab, qui est un côté des deux Q et R. Notez que $3 \leq s \leq k$ et $3 \leq t \leq k$ car les deux Q et R ont au moins un côté de moins que P (après tout, chacun d'eux est formé de P en supprimant au moins deux côtés et en remplaçant ces côtés par la diagonale ab). En outre, le nombre de côtés de P est deux de moins que la somme des nombres de côtés de Q et du nombre de

Épisode 361

une

b T e *T* est le triangle *abc*

p *p* est le sommet de *P à l'* intérieur de *T* tel que le *bap* est le plus petit

g *bp* doit être une diagonale intérieure de *P*

q F ré

P

c

FIGURE 3 **Construction d'une diagonale intérieure d'un polygone simple.**

côtés de R, parce que chaque côté de P est un côté de Q ou de R, mais pas les deux, et la diagonale ab est une vue latérale des deux Q et R, mais pas P. Autrement dit, $k + 1 = s + t - 2$.

Nous utilisons maintenant l'hypothèse inductive. Parce que $3 \leq s \leq k$ et $3 \leq t \leq k$, par l'inductance hypothèse positive, nous pouvons trianguler Q et R en triangles s - 2 et t - 2, respectivement. Prochain, A noter que ces triangulations produisent ensemble une triangulation de P. (Chaque diagonale ajoutée à trianguler un de ces petits polygones est également une diagonale de P.) Par conséquent, nous pouvons trian-calculer P en un total de $(s - 2) + (t - 2) = s + t - 4 = (k + 1) - 2$ triangles. Ceci termine la preuve par forte induction. Autrement dit, nous avons montré que chaque polygone simple avec n côtés, où $n \geq 3$, peut être triangulé en $n - 2$ triangles.

Nous revenons maintenant à notre preuve du lemme 1. Nous présentons une preuve publiée par Chung-Wu Ho [Ho75]. Notez que bien que cette preuve puisse être omise sans perte de continuité, elle fournit une preuve correcte d'un résultat prouvé incorrectement par de nombreux mathématiciens.

Preuve: Supposons que P est un simple polygone dessiné dans le plan. De plus, supposons que b soit le point de P ou à l'intérieur de P avec le moins y coordonné parmi les sommets avec le plus petite coordonnée x. Alors b doit être un sommet de P, car s'il s'agit d'un point intérieur, il y aurait doivent être un sommet de P avec une coordonnée x plus petite. Deux autres sommets partagent chacun une arête avec b, disons a et c. Il s'ensuit que l'angle à l'intérieur de P formé par ab et bc doit être moins de 180 degrés (sinon, il y aurait des points de P avec des coordonnées x plus petites que b).

Soit maintenant T le triangle $\triangle abc$. S'il n'y a pas de sommets de P sur ou à l'intérieur de T, nous pouvons reliez a et c pour obtenir une diagonale intérieure. Par contre, s'il y a des sommets de P à l'intérieur de T, nous trouverons un sommet p de P sur ou à l'intérieur de T tel que bp soit une diagonale intérieure. (Cette est la partie délicate. Ho a noté que dans de nombreuses preuves publiées de ce lemme, un sommet p a été trouvé de telle sorte que pb était pas nécessairement une diagonale intérieure de P. Voir exercice 21.) La clé est de sélectionnez un sommet p tel que l'angle Z bap soit le plus petit. Pour voir cela, notez que le rayon commençant en a et en passant par p frappe le segment de ligne bc en un point, disons q. Il s'ensuit alors que le le triangle $\triangle baq$ ne peut contenir aucun sommet de P à l'intérieur. Par conséquent, nous pouvons relier b et p pour produire une diagonale intérieure de P. La localisation de ce sommet p est illustrée à la figure 3.

Preuves à l'aide de la propriété Well-Ordering

La validité du principe de l'induction mathématique et de l'induction forte découle de un axiome fondamental de l'ensemble des entiers, la **propriété de bon ordre** (voir annexe 1). le la propriété bien ordonnée indique que chaque ensemble non vide d'entiers non négatifs a un moindre élément. Nous montrerons comment la propriété de bon ordre peut être utilisée directement dans les épreuves En outre, il peut être démontré (voir exercices 41, 42 et 43) que la propriété de bon ordre, le principe de l'induction mathématique et l'induction forte sont toutes équivalentes. Autrement dit, la validité de chacun des ces trois techniques de preuve impliquent la validité des deux autres techniques. Dans la section 5.1, nous

ont montré que le principe de l'induction mathématique découle de la propriété de bon ordre. Les autres parties de cette équivalence restent les exercices 31, 42 et 43.

LA PROPRIÉTÉ DU BIEN-ORDRE Chaque ensemble non vide d'entiers non négatifs a un moindre élément.

La propriété bien ordonnée peut souvent être utilisée directement dans les épreuves.

EXEMPLE 5 Utilisez la propriété well-ordering pour prouver l'algorithme de division. Rappelons que l'algorithme de division indique que si a est un entier et d est un entier positif, alors il y a des entiers uniques q et r avec $0 \leq r < d$ et $a = dq + r$.

Solution: Soit S l'ensemble des entiers non négatifs de la forme $a - dq$, où q est un entier. Cette set est non vide parce que $-dq$ peut être rendu aussi grand que souhaité (en prenant q pour être un entier négatif avec une grande valeur absolue). Par la propriété bien ordonnée, S a au moins un élément $r = a - dq_0$.

L'entier r est non négatif. Il est également vrai que $r < d$. Sinon, il y aurait être un élément non négatif plus petit dans S, à savoir, $a - d(q_0 + 1)$. Pour voir cela, supposons que $r \geq d$. Parce *que* $a = dq_0 + r$, il s'ensuit que $a - d(q_0 + 1) = (a - dq_0) - d = r - d \geq 0$. Conse-par conséquent, il existe des entiers q et r avec $0 \leq r < d$. La preuve que q et r sont uniques est laissée comme Exercice 37. ▲

EXEMPLE 6 Dans un tournoi à la ronde, chaque joueur joue tous les autres joueurs exactement une fois et à chaque match a un gagnant et un perdant. On dit que les joueurs $p_1, p_2, \ldots, p_m$ forment un *cycle* si p_1 bat p_2, p_2 bat p_3, ..., p_{m-1} bat p_m et p_m bat p_1. Utilisez le principe du bon ordre pour montrer que si il y a un cycle de longueur m $(m \geq 3)$ parmi les joueurs d'un tournoi à la ronde, il faut être un cycle de trois de ces joueurs.

Solution: Nous supposons qu'il n'y a pas de cycle de trois joueurs. Parce qu'il y a au moins un cycle dans le tournoi à la ronde, l'ensemble de tous les entiers positifs n pour lesquels il existe un cycle de la longueur n n'est pas vide. Par la propriété de bon ordre, cet ensemble d'entiers positifs a au moins élément k, qui par hypothèse doit être supérieur à trois. Par conséquent, il existe un cycle des joueurs $p_1, p_2, p_3, \ldots, p_k$ et aucun cycle plus court n'existe.

Parce qu'il n'y a pas de cycle de trois joueurs, nous savons que $k > 3$. Considérez les trois premiers éléments de ce cycle, p_1, p_2 et p_3. Il y a deux résultats possibles de la correspondance entre p_1 et p_3. Si p_3 bat p_1, il s'ensuit que p_1, p_2, p_3 est un cycle de longueur trois, en contradiction avec notre hypothèse qu'il n'y a pas de cycle de trois joueurs. Par conséquent, il doit être vrai que p_1 bat p_3. Cela signifie que nous pouvons omettre p_2 du cycle $p_1, p_2, p_3, \ldots, p_k$ pour obtenir le cycle p_1, p_3, p_4, ..., p_k de longueur k - 1, contredisant l'hypothèse que le plus petit cycle a une longueur k. Nous concluons qu'il doit y avoir un cycle de longueur trois. ▲

Des exercices

1. Utilisez une forte induction pour montrer que si vous pouvez courir un mile ou deux miles, et si vous pouvez toujours courir deux miles de plus une fois que vous avez parcouru un nombre spécifié de miles, vous peut parcourir n'importe quel nombre de miles.

2. Utilisez une forte induction pour montrer que tous les dominos tombent disposition infinie de dominos si vous savez que le les trois premiers dominos tombent, et que lorsqu'un domino tombe, le domino trois plus bas dans l'arrangement aussi chutes.

3. Soit $P(n)$ la déclaration selon laquelle un affranchissement de n cents peut être formé en utilisant seulement des timbres de 3 cents et des timbres de 5 cents. le certaines parties de cet exercice décrivent une forte preuve d'induction $P(n)$ est vrai pour $n \geq 8$.

a) Montrer que les énoncés $P(8)$, $P(9)$ et $P(10)$ sont vrai, complétant l'étape de base de la preuve.

b) Quelle est l'hypothèse inductive de la preuve?

c) Que devez-vous prouver dans l'étape inductive?

d) Complétez l'étape inductive pour $k \geq 10$.

e) Expliquez pourquoi ces étapes montrent que cette déclaration est vrai chaque fois que $n \geq 8$.

4. Soit $P(n)$ la déclaration selon laquelle un affranchissement de n cents peut être formé en utilisant seulement des timbres de 4 cents et des timbres de 7 cents. le

certaines parties de cet exercice décrivent une forte preuve d'induction $P(n)$ est vrai pour $n \geq 18$.

a) Afficher les déclarations $P(18)$, $P(19)$, $P(20)$ et $P(21)$ sont vraies, complétant l'étape de base de la preuve.

b) Quelle est l'hypothèse inductive de la preuve?

c) Que devez-vous prouver dans l'étape inductive?

d) Complétez l'étape inductive pour $k \geq 21$.

e) Expliquez pourquoi ces étapes montrent que cette déclaration est vrai chaque fois que $n \geq 18$.

5. a) Déterminer quels montants d'affranchissement peuvent être formés en utilisant seulement des timbres de 4 et 11 cents.

b) Démontrez votre réponse à (a) en utilisant le principe de induction ématique. Assurez-vous d'indiquer explicitement votre hypothèse inductive dans l'étape inductive.

c) Prouve ta réponse à (a) en utilisant une forte induction. Comment l'hypothèse inductive de cette preuve diffère-t-elle de que dans l'hypothèse inductive d'une preuve utilisant des induction ématique?

6. a) Déterminer quels montants d'affranchissement peuvent être formés en utilisant seulement des timbres de 3 et 10 cents.

b) Démontrez votre réponse à (a) en utilisant le principe de induction ématique. Assurez-vous d'indiquer explicitement votre hypothèse inductive dans l'étape inductive.

c) Prouve ta réponse à (a) en utilisant une forte induction. Comment l'hypothèse inductive de cette preuve diffère-t-elle de que dans l'hypothèse inductive d'une preuve utilisant des induction ématique?

7. Quels montants d'argent peuvent être formés en utilisant billets d'un dollar et billets de cinq dollars? Prouvez votre réponse en utilisant forte induction.

8. Supposons qu'un magasin propose des chèques-cadeaux en 25 dollars et 40 dollars. Déterminer le possible les montants totaux que vous pouvez former en utilisant ces certificats-cadeaux. Prouvez votre réponse en utilisant une forte induction.

∗ **9.** Utilisez une forte induction pour prouver que $\sqrt{2}$ est irrationnel. [*Indice:* Soit $P(n)$ la déclaration que $\sqrt{2} = n / b$ pour tout positif entier b.]

10. Supposons qu'une barre de chocolat se compose de n carrés rangé dans un motif rectangulaire. L'ensemble du bar, un plus petit pièce rectangulaire de la barre, peut être brisée le long d'une verticale ou une ligne horizontale séparant les carrés. En admettant que une seule pièce peut être cassée à la fois, déterminez comment de nombreuses pauses à faire successivement pour briser la barre en n carrés séparés. Utilisez une forte induction pour prouver Ta Réponse.

11. Considérez cette variante du jeu de Nim. Le jeu commence par n correspondances. Deux joueurs se relaient à tour de rôle correspond à un, deux ou trois à la fois. Le joueur enlève le dernier match perd. Utilisez une forte induction pour montrer que si chaque joueur joue la meilleure stratégie possible, le le premier joueur gagne si $n = 4j$, $4j + 2$ ou $4j + 3$ pour certains

12. Utilisez une forte induction pour montrer que chaque entier positif n peut être écrit comme une somme de deux pouvoirs distincts, c'est-à-dire comme la somme d'un sous-ensemble des entiers $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, etc. [*Astuce:* pour l'étape inductive, séparément considérons le cas où $k + 1$ est pair et où il est impair. Quand il est pair, notez que $(k + 1) / 2$ est un entier.]

∗ **13.** Un puzzle est constitué en se joignant successivement pièces qui s'emboîtent en blocs. Un mouvement est fait chacun moment où une pièce est ajoutée à un bloc, ou lorsque deux blocs sont joints. Utilisez une forte induction pour prouver que peu importe comment les mouvements sont effectués, exactement n - 1 mouvements sont nécessaire pour assembler un puzzle avec n pièces.

14. Supposons que vous commenciez par un tas de n pierres et que vous empiler en n tas d'une pierre chacun en divisant successivement ting un tas de pierres en deux plus petits tas. Chaque fois que vous diviser une pile, vous multipliez le nombre de pierres dans chaque des deux plus petits tas que vous formez, de sorte que si ces tas ont des pierres r et s, respectivement, vous calculez rs. Montrez que peu importe comment vous divisez les piles, la somme des produits calculés à chaque étape est égal à $n(n - 1) / 2$.

15. Montrer que le premier joueur a une stratégie gagnante pour le jeu de Chomp, présenté dans l'exemple 12 de la section 1.8, si la planche initiale est carrée. [*Astuce:* utilisez une forte induction pour montrer que cette stratégie fonctionne. Pour le premier mouvement, le le premier joueur ébrèche tous les cookies sauf ceux de gauche et bords supérieurs. Lors des coups suivants, après le deuxième joueur a haché des cookies sur le bord supérieur ou gauche, le le premier joueur ébrèche les cookies dans les mêmes positions relatives dans le bord gauche ou supérieur, respectivement.]

∗ **16.** Prouver que le premier joueur a une stratégie gagnante pour le jeu de Chomp, présenté dans l'exemple 12 de la section 1.8, si la planche initiale est large de deux carrés, c'est-à-dire un $2 \times n$ planche. [*Astuce:* utilisez une forte induction. Le premier mouvement du le premier joueur devrait être de casser le cookie dans le fond ligne à l'extrême droite.]

17. Utilisez une forte induction pour montrer que si un simple polygone avec au moins quatre côtés est triangulé, puis au moins deux des triangles de la triangulation ont deux côtés qui borde l'extérieur du polygone.

∗ **18.** Utilisez une forte induction pour montrer que lorsqu'un simple gon P avec des sommets consécutifs v_1, v_2, ..., v_n est trian- divisé en n - 2 triangles, les n - 2 triangles peuvent être numérotés 1, 2, ..., n - 2 de sorte que v_i soit un sommet de triangle i pour i = 1, 2, ..., n - 2.

∗ **19. Le théorème de Pick** dit que l'aire d'un poly- gon P dans le plan avec des sommets qui sont tous en treillis points (c'est-à-dire des points avec des coordonnées entières) est égal à $I(P) + B(P) / 2 - 1$, où $I(P)$ et $B(P)$ sont les nombre de points de réseau à l'intérieur de P et sur le limite de P, respectivement. Utilisez une forte induction sur le nombre de sommets de P pour prouver le théorème de Pick. [*Indice:* Pour l'étape de base, prouver d'abord le théorème des rectangles, puis pour les triangles rectangles, et enfin pour tous les triangles par notant que l'aire d'un triangle est l'aire d'un plus grand entier non négatif j et le deuxième joueur gagne dans le cas restant lorsque $n = 4j + 1$ pour certains non négatifs entier j.

rectangle le contenant avec les aires d'au plus trois triangles soustraits. Pour l'étape inductive, profitez du lemme 1.]

Épisode 364

∗∗ 20. Supposons que P soit un simple polygone avec des sommets $v_1, v_2, \ldots, v_n$ énumérés de façon à ce que les sommets consécutifs soient con- connectés par une arête, et v_1 et v_n sont reliés par une arête. Un sommet v_i est appelé une **oreille** si le segment de ligne se connectant les deux sommets adjacents à v_i est une diagonale intérieure du polygone simple. Deux oreilles v_i et v_j sont appelées **non clapotis** si l'intérieur des triangles à sommets v_i et ses deux sommets adjacents et v_j et ses deux adjacents les sommets ne se coupent pas. Prouver que chaque polygone simple avec au moins quatre sommets a au moins deux non superposés oreilles.

21. Dans la preuve du lemme 1, nous avons mentionné que de bonnes méthodes pour trouver un sommet p tel que le segment de ligne bp est une diagonale intérieure de P ont été publié. Cet exercice présente certaines des erreurs des moyens p a été choisi dans ces épreuves. Afficher, par con- en considérant l'un des polygones dessinés ici, celui de chacun ces choix de p, le segment de ligne bp n'est pas nécessairement une diagonale intérieure de P.

a) p est le sommet de P tel que l'angle $\angle abp$ soit petit- est.

b) p est le sommet de P avec la coordonnée la moins x (autre que b).

c) p est le sommet de P *le* plus proche de b.

une *une* *b* *p* *F* *q* *b* *g* *p* *s* *r* *c* *ré* *h* *c* *e*

Les exercices 22 et 23 présentent des exemples qui montrent la charge peut être utilisée pour prouver les résultats de la etry.

∗ 22. Soit $P(n)$ l'affirmation selon laquelle, lors de la di- les agonales sont dessinées à l'intérieur d'un polygone convexe à n côtés, au moins deux sommets du polygone ne sont pas des extrémités de l'une de ces diagonales.

a) Montrer que lorsque nous essayons de prouver $P(n)$ pour tous les gers n avec $n \geq 3$ en utilisant une forte induction, l'inductive l'étape ne passe pas.

b) Montrer que nous pouvons prouver que $P(n)$ est vrai pour tous les gers n avec $n \geq 3$ en prouvant par forte induction la assertion $Q(n)$ plus forte, pour $n \geq 4$, où $Q(n)$ indique que chaque fois que des diagonales sans intersection sont dessinées côté un polygone convexe avec n côtés, au moins deux *non les* sommets *adjacents* ne sont pas des extrémités de ces diagonales.

23. Soit $E(n)$ l'affirmation selon laquelle dans une triangulation d'une sim- plein polygone avec n côtés, au moins un des triangles la triangulation a deux côtés bordant l'extérieur de le polygone.

a) Expliquez où une preuve utilisant une forte induction qui $E(n)$ est vrai pour tous les entiers $n \geq 4$ rencontre des difficultés.

b) Montrer que nous pouvons prouver que $E(n)$ est vrai pour tous les gers $n \geq 4$ en prouvant par forte induction, le plus fort déclaration $T(n)$ pour tous les entiers $n \geq 4$, qui indique que dans chaque triangulation d'un polygone simple, au moins deux des triangles de la triangulation ont deux côtés bor- à l'extérieur du polygone.

∗ 24. Une affectation stable, définie dans le préambule de Cise 60 à la section 3.1, est appelée **optimale pour soupirants** si aucune affectation stable existe dans laquelle un prétendant est jumelé avec une suite que ce prétendant préfère à la personne à qui ce prétendant est jumelé dans cette affectation stable. Utilisez fort induction pour montrer que l'algorithme d'acceptation différée produit une affectation stable qui est optimale pour les prétendants.

25. Supposons que $P(n)$ soit une fonction propositionnelle. Déterminer pour lesquels des entiers positifs n l'instruction $P(n)$ doit être vrai, et justifier votre réponse, si

a) $P(1)$ est vrai; pour tous les entiers positifs n, si $P(n)$ est vrai, alors $P(n+2)$ est vrai.

b) $P(1)$ et $P(2)$ sont vrais; pour tous les entiers positifs n, si $P(n)$ et $P(n+1)$ sont vrais, alors $P(n+2)$ est vrai.

c) $P(1)$ est vrai; pour tous les entiers positifs n, si $P(n)$ est vrai, alors $P(2n)$ est vrai.

d) $P(1)$ est vrai; pour tous les entiers positifs n, si $P(n)$ est vrai, alors $P(n+1)$ est vrai.

26. Supposons que $P(n)$ soit une fonction propositionnelle. Déterminer pour lesquels entiers non négatifs n l'instruction $P(n)$ doit être vrai si

a) $P(0)$ est vrai; pour tous les entiers non négatifs n, si $P(n)$ est vrai, alors $P(n+2)$ est vrai.

b) $P(0)$ est vrai; pour tous les entiers non négatifs n, si $P(n)$ est vrai, alors $P(n+3)$ est vrai.

c) $P(0)$ et $P(1)$ sont vrais; pour tous les entiers non négatifs n, si $P(n)$ et $P(n+1)$ sont vrais, alors $P(n+2)$ est vrai.

d) $P(0)$ est vrai; pour tous les entiers non négatifs n, si $P(n)$ est vrai, alors $P(n+2)$ et $P(n+3)$ sont vrais.

27. Montrer que si l'énoncé $P(n)$ est vrai pour une infinité de entiers positifs n et $P(n+1) \rightarrow P(n)$ est vrai pour tous entiers positifs n, alors $P(n)$ est vrai pour tous les entiers positifs gers n.

28. Soit b un entier fixe et j un entier positif fixe ger. Montrer que si $P(b), P(b+1), \ldots, P(b+j)$ sont vrais et $[P(b) \wedge P(b+1) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ est vrai pour chaque entier $k \geq b+j$, alors $P(n)$ est vrai pour tous entiers n avec $n \geq b$.

29. Quel est le problème avec cette «preuve» par induction forte?

«Théorème» Pour tout entier non négatif n, $5n = 0$.

Étape de base: $5 \cdot 0 = 0$.

Étape inductive: supposons que $5j = 0$ pour tous les nonneg- entiers actifs j avec $0 \leq j \leq k$. Écrivez $k+1 = i+j$, où i et j sont des nombres naturels inférieurs à $k+1$. Par le hypothèse inductive, $5(k+1) = 5(i+j) = 5i + 5j = 0 + 0 = 0$.

∗ **30.** Trouver la faille avec les éléments suivants « preuve » que d' $un_n = 1$ pour tous les entiers non négatifs n, chaque fois *que* a est un réel non nul nombre.

Étape de base: $un_0 = 1$ est vrai par la définition d' un_0.

Étape inductive: Supposons que $a_j = 1$ pour tout non négatif entiers j avec $j \leq k$. Notez ensuite que

$$a_{k+1} = \frac{a_k \cdot a_k}{a_{k-1}} = \frac{1 \cdot 1}{1} = 1 .$$

∗ **31.** Montrer qu'une forte induction est une méthode de preuve valable en montrant qu'il découle de la propriété bien ordonnée.

32. Trouvez la faille avec la «preuve» suivante que chaque l'affranchissement de trois cents ou plus peut être formé en utilisant juste timbres de trois cents et quatre cents.

Étape de base: Nous pouvons former un affranchissement de trois cents avec un timbre unique de trois cents et nous pouvons former l'affranchissement de quatre cents en utilisant un seul timbre de quatre cents.

Étape inductive: Supposons que nous pouvons former un affranchissement de j cents pour tous les entiers non négatifs j avec $j \leq k$ us- avec seulement trois cents et quatre cents. On peut alors former un affranchissement de $k + 1$ cents en remplaçant un trois cents timbre avec un timbre de quatre cents ou en remplaçant deux timbres de cent par trois timbres de trois cents.

33. Montrer que nous pouvons prouver que $P(n, k)$ est vrai pour toutes les paires d'entiers positifs n et k si nous montrons

a) $P(1, 1)$ est vrai et $P(n, k) \rightarrow [P(n + 1, k) \wedge P(n, k + 1)]$ est vrai pour tous les entiers positifs n et k.

b) $P(1, k)$ est vrai pour tous les entiers positifs k, et $P(n, k) \rightarrow P(n + 1, k)$ est vrai pour tous les positifs gers n et k.

c) $P(n, 1)$ est vrai pour tous les entiers positifs n, et $P(n, k) \rightarrow P(n, k + 1)$ est vrai pour tous les positifs gers n et k.

34. Prouver que $\sum_{j=1}^{n} j(j + 1)(j + 2) \cdots (j + k - 1) = n(n + 1)(n + 2) \cdots (n + k) / (k + 1)$ pour tous les positifs gers k et n. [*Astuce* : utilisez une technique de l'exercice 33.]

∗ **35.** Montrer que si $a_1, a_2, \ldots, a_n$ sont n nombres réels distincts, ex- en fait $n - 1$ multiplications sont utilisées pour calculer le uct de ces n nombres, peu importe la façon dont les parenthèses sont inséré dans leur produit. [*Astuce:* utilisez une forte induction et considérez la dernière multiplication.]

∗ **36.** La propriété bien ordonnée peut être utilisée pour montrer qu'il est le plus grand diviseur commun unique de deux tegers. Soit a et b des entiers positifs, et soit S soit l'ensemble des entiers positifs de la forme *comme* + bt, où s et t sont des entiers.

a) Montrez que S n'est pas vide.

b) Utilisez la propriété de bon ordre pour montrer que S a un le plus petit élément c.

c) Montrer que si d est un diviseur commun de a et b, alors d est un diviseur de c.

d) Montrer que $c \mid a$ et $c \mid b$. [*Astuce:* Tout d'abord, supposez que $c \mid a$. Alors $a = qc + r$, où $0 < r < c$. Montre CA $r \in S$, contredisant le choix de c.]

e) conclure des points c) et d) que la plus grande commune il existe *un* diviseur de a et b. Terminez l'épreuve en montrant que ce plus grand diviseur commun est unique.

37. Soit a un entier et d un entier positif. Spectacle que les entiers q et r avec $a = dq + r$ et $0 \leq r < d$, qui se sont avérées exister dans l'exemple 5, sont uniques.

38. Utilisez l'induction mathématique pour montrer qu'un damier lar avec un nombre pair de cellules et deux carrés manquants, un blanc et un noir, peuvent être couverts par des dominos.

∗∗ **39.** Pouvez-vous utiliser la propriété bien ordonnée pour prouver ment: «Chaque entier positif peut être décrit en utilisant plus de quinze mots anglais »? Supposons les mots provenir d'un dictionnaire particulier de l'anglais. [*Indice:* sup- posent qu'il existe des entiers positifs qui ne peuvent pas être dé- écrit en utilisant pas plus de quinze mots anglais. Par bien ordonné, *le plus petit entier positif qui ne peut pas être décrit en utilisant pas plus de quinze mots anglais* existerait alors.]

40. Utilisez le principe de bon ordre pour montrer que si x et y sont des nombres réels avec $x < y$, alors il y a un rationnel nombre r avec $x < r < y$. [*Astuce:* utilisez l'archimède donnée à l'appendice 1 pour trouver un résultat positif entier A avec $A > 1 / (y - x)$. Montrez ensuite qu'il y a un nombre rationnel r avec le dénominateur A entre x et y en regardant les nombres $\lfloor x \rfloor + j / A$, où j est un entier positif.]

∗ **41.** Montrer que la propriété de bon ordre peut être prouvée lorsque le principe de l'induction mathématique est pris comme iom.

∗ **42.** Montrer que le principe de l'induction mathématique et une forte induction est équivalente; c'est-à-dire que chacun peut être montré être valable de l'autre.

∗ **43.** Montrez que nous pouvons prouver la propriété bien ordonnée lorsque nous prenons une forte induction comme axiome au lieu de prendre la propriété bien ordonnée comme axiome.

Définitions récursives et induction structurelle

introduction

Parfois, il est difficile de définir explicitement un objet. Cependant, il peut être facile de définir ce objet en termes de lui-même. Ce processus est appelé **récursivité**. Par exemple, l'image montrée dans La figure 1 est produite de manière récursive. Tout d'abord, une photo originale est donnée. Puis un processus de successivement une superposition d'images plus petites centrées sur les images précédentes est effectuée.

FIGURE 1 **Une image définie récursivement.**

Nous pouvons utiliser la récursivité pour définir des séquences, des fonctions et des ensembles. Dans la section 2.4, et dans la plupart début des cours de mathématiques, les termes d'une séquence sont spécifiés à l'aide d'une formule explicite. Par exemple, la séquence de puissances de 2 est donnée par $un_n = 2^n$ pour $n = 0, 1, 2, \ldots$. Rappel de Section 2.4 que nous pouvons également définir une séquence récursivement en spécifiant comment les termes de la séquence sont trouvés à partir des termes précédents. La séquence de puissances de 2 peut également être définie en donnant le premier terme de la séquence, à savoir $un_0 = 1$, et une règle pour trouver un terme du séquence de la précédente, à savoir, $a_{n+1} = 2a_n$ pour $n = 0, 1, 2, \ldots$. Lorsque nous définissons un séquence récursivement en spécifiant comment les termes de la séquence sont trouvés à partir des termes précédents, nous pouvons utiliser l'induction pour prouver les résultats de la séquence.

Lorsque nous définissons un ensemble récursivement, nous spécifions certains éléments initiaux dans une étape de base et fournir une règle pour construire de nouveaux éléments à partir de ceux que nous avons déjà étape progressive. Pour prouver les résultats sur les ensembles définis récursivement, nous utilisons une méthode appelée ***structurelle induction*** .

Fonctions définies de manière récursive

Nous utilisons deux étapes pour définir une fonction avec l'ensemble d'entiers non négatifs comme domaine:

ÉTAPE DE BASE: Spécifiez la valeur de la fonction à zéro.

ÉTAPE Récursive: Donnez une règle pour trouver sa valeur à un entier à partir de ses valeurs à plus petit entiers.

Une telle définition est appelée définition **récursive** ou **inductive** . Notez qu'une fonction $f(n)$ de l'ensemble des entiers non négatifs à l'ensemble des nombres réels est le même qu'une séquence $a_0, a_1, \ldots$ où a_i est un nombre réel pour chaque entier non négatif i . Donc, définir une séquence à valeur réelle $a_0, a_1, \ldots$ *en* utilisant une relation de récurrence, comme cela a été fait dans la section 2.4, revient à définir un fonction de l'ensemble des entiers non négatifs à l'ensemble des nombres réels.

EXEMPLE 1 Supposons que f soit défini récursivement par

$$f(0) = 3,$$
$$f(n+1) = 2f(n) + 3.$$

Trouvez $f(1)$, $f(2)$, $f(3)$ et $f(4)$.

Solution: de la définition récursive, il s'ensuit que

$$f(1) = 2f(0) + 3 = 2 \cdot 3 + 3 = 9,$$
$$f(2) = 2f(1) + 3 = 2 \cdot 9 + 3 = 21,$$
$$f(3) = 2f(2) + 3 = 2 \cdot 21 + 3 = 45,$$
$$f(4) = 2f(3) + 3 = 2{,}45 + 3 = 93.$$

▲

Les fonctions définies de manière récursive sont **bien définies** . Autrement dit, pour chaque entier positif, le La valeur de la fonction à cet entier est déterminée sans ambiguïté.Ça signifie étant donné tout entier positif, nous pouvons utiliser les deux parties de la définition pour trouver la valeur de la fonction à cet entier, et que nous obtenons la même valeur, peu importe comment nous l'appliquons appliquer les deux parties de la définition.Ceci est une conséquence du principe de induction cal. (Voir exercice 56.) D'autres exemples de définitions récursives sont donnés dans Exemples 2 et 3.

EXEMPLE 2 Donner une définition récursive d' un_n, où a est un nombre réel non nul et n est un nombre non négatif entier.

Solution: la définition récursive contient deux parties. D'abord, un_0 est spécifié, à savoir, $un_0 = 1$. Ensuite la règle pour trouver un_{n+1} d' un_n, à savoir, $a_{n+1} = a \cdot a_n$, pour $n = 0, 1, 2, 3, \ldots$, est donné. Celles-ci deux équations définissent uniquement un_n pour tous les entiers non négatifs n.

▲

EXEMPLE 3 Donnez une définition récursive de

$$\sum_{k=0}^{n} a_k.$$

Solution: la première partie de la définition récursive est

$$\sum_{k=0}^{0} a_k = a_0.$$

La deuxième partie est

$$\sum_{k=0}^{n+1} a_k = \left(\sum_{k=0}^{n} un_k\right) + a_{n+1}.$$

▲

Dans certaines définitions récursives de fonctions, les valeurs de la fonction au premier k positif des entiers sont spécifiés et une règle est donnée pour déterminer la valeur de la fonction à des gers à partir de ses valeurs à tout ou partie des k entiers précédents . Que les définitions récursives définies produire ainsi des fonctions bien définies découle d'une forte induction (voir exercice 57).

Épisode 368

Rappelons à la section 2.4 que les nombres de Fibonacci, $f_0, f_1, f_2, \ldots$, sont définis par le équations $f_0 = 0$, $f_1 = 1$, et

$$f_n = f_{n-1} + f_{n-2}$$

pour $n = 2, 3, 4, \ldots$. [On peut penser au nombre de Fibonacci f_n soit comme le n ème terme du séquence de nombres de Fibonacci $f_0, f_1, \ldots$ ou comme valeur à l'entier n d'une fonction $f(n)$.]

Nous pouvons utiliser la définition récursive des nombres de Fibonacci pour prouver de nombreuses propriétés de ces chiffres. Nous donnons une telle propriété dans l'exemple 4.

EXEMPLE 4 Montrer que chaque fois que $n \geq 3$, $f_n > \alpha^{n-2}$, où $\alpha = (1 + \sqrt{5})/2$.

Solution: Nous pouvons utiliser une forte induction pour prouver cette inégalité. Soit $P(n)$ la déclaration $f_n > \alpha^{n-2}$. Nous voulons montrer que $P(n)$ est vrai chaque fois que n est un entier supérieur ou égal à 3.

ÉTAPE DE BASE: Tout d'abord, notez que

$$\alpha < 2 = f_3, \qquad \alpha^2 = (3 + \sqrt{5})/2 < 3 = f_4,$$

donc $P(3)$ et $P(4)$ sont vrais.

ÉTAPE INDUCTIVE: Supposons que $P(j)$ soit vrai, à savoir que $f_j > \alpha^{j-2}$, pour tous les entiers j avec $3 \leq j \leq k$, où $k \geq 4$. Nous devons montrer que $P(k+1)$ est vrai, c'est-à-dire que $f_{k+1} > \alpha^{k-1}$. Car α est une solution de $x^2 - x - 1 = 0$ (comme le montre la formule quadratique), il s'ensuit que $\alpha^2 = \alpha + 1$. Donc,

$$\alpha^{k-1} = \alpha^2 \cdot \alpha^{k-3} = (\alpha + 1)\alpha^{k-3} = \alpha \cdot \alpha^{k-3} + 1 \cdot \alpha^{k-3} = \alpha^{k-2} + \alpha^{k-3}.$$

Par l'hypothèse inductive, car $k \geq 4$, nous avons

$$f_{k-1} > \alpha^{k-3}, \qquad f_k > \alpha^{k-2}.$$

Il s'ensuit donc que

$$f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}.$$

Par conséquent, $P(k+1)$ est vrai. Ceci complète la preuve. ▲

Remarque: L'étape inductive montre que chaque fois que $k \geq 4$, $P(k+1)$ découle de l'hypothèse que $P(j)$ est vrai pour $3 \leq j \leq k$. Par conséquent, l'étape inductive ne montre *pas* que $P(3) \to P(4)$. Par conséquent, nous avons dû montrer que $P(4)$ est vrai séparément.

Nous pouvons maintenant montrer que l'algorithme euclidien, introduit dans la section 4.3, utilise $O(\log b)$ divisions pour trouver le plus grand diviseur commun des entiers positifs a et b, où $a \geq b$.

THÉORÈME 1 **LE THÉORÈME DE LAMÉ** Soit a et b des entiers positifs avec $a \geq b$. Ensuite, le nombre de les divisions utilisées par l'algorithme euclidien pour trouver le pgcd (a, b) est inférieure ou égale à cinq fois le nombre de chiffres décimaux en b.

Preuve: Rappelons que lorsque l'algorithme euclidien est appliqué pour trouver gcd (a, b) avec $a \geq b$, ce on obtient une séquence d'équations (où $a = r_0$ et $b = r_1$).

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2,\\
&\ \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_n.
\end{aligned}$$

Ici, n divisions ont été utilisées pour trouver $r_n =$ pgcd (a, b). Notez que les quotients $q_1, q_2, \ldots, q_{n-1}$ sont tous au moins 1. De plus, $q_n \geq 2$, car $r_n < r_{n-1}$. Ceci implique que

$$r_n \geq 1 = f_2,$$
$$r_{n-1} \geq 2r_n \geq 2f_2 = f_3,$$

$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4$,

.
.
.

$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n$,

$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}$.

Il s'ensuit que si n divisions sont utilisées par l'algorithme euclidien pour trouver gcd (a, b) avec $a \geq b$, alors $b \geq f_{n+1}$. Par l'exemple 4, nous savons que $f_{n+1} > \alpha^{n-1}$ pour $n > 2$, où $\alpha = (1 + \sqrt{5})/2$. Il s'ensuit donc que $b > \alpha^{n-1}$. De plus, car $\log_{10} \alpha \approx 0.208 > 1/5$, nous voyons que

$$\log_{10} b > (n-1) \log_{10} \alpha > (n-1)/5 .$$

Par conséquent, $n - 1 < 5 \cdot \log_{10} b$. Supposons maintenant que b ait k chiffres décimaux. Alors $b < 10^k$ et $\log_{10} b < k$. Il s'ensuit que $n - 1 < 5k$, et parce que k est un entier, il s'ensuit que $n \leq 5k$. Ceci termine la preuve.

Parce que le nombre de chiffres décimaux en b, qui est égal à $\lfloor \log_{10} b \rfloor + 1$, est inférieur ou égal pour $\log_{10} b + 1$, le théorème 1 nous dit que le nombre de divisions nécessaires pour trouver pgcd(a, b) avec

FIBONACCI (1170-1250) Fibonacci (abréviation de *filius Bonacci,* ou «fils de Bonacci») était également connu sous le nom de Léonard de Pise. Il est né dans le centre commercial italien de Pise. Fibonacci était un marchand qui voyageait largement à travers le Moyen-Orient, où il est entré en contact avec les mathématiques arabes. Dans son livre *Liber Abaci,* Fibonacci a introduit le monde européen à la notation arabe pour les chiffres et les algorithmes pour l'arithmétique. C'est dans ce livre que son fameux problème de lapin (décrit dans la section 8.1) est apparu. Fibonacci a également écrit livres sur la géométrie et la trigonométrie et sur les équations diophantiennes, qui impliquent de trouver des solutions entières à équations.

$a > b$ est inférieur ou égal à $5(\log_{10} b + 1)$. Parce que $5(\log_{10} b + 1)$ est $O(\log b)$, nous voyons que *Les* divisions $O(\log b)$ sont utilisées par l'algorithme euclidien pour trouver gcd (a, b) chaque fois *que* $a > b$.

Ensembles et structures définis de manière récursive

Nous avons exploré comment les fonctions peuvent être définies récursivement. Nous tournons maintenant notre attention vers la façon dont les ensembles peut être défini récursivement. Tout comme dans la définition récursive des fonctions, les définitions récursives des ensembles ont deux parties, une **étape de base** et une **étape récursive**. Dans l'étape de base, une première collecte des éléments est spécifié. À l'étape récursive, les règles de formation de nouveaux éléments dans l'ensemble à partir de ceux déjà connus pour être dans l'ensemble sont fournis. Les définitions récursives peuvent également inclure un **règle d'exclusion**, qui spécifie qu'un ensemble défini récursivement ne contient rien d'autre que ceux les éléments spécifiés dans l'étape de base ou générés par les applications de l'étape récursive. Dans notre discussions, nous supposerons toujours tacitement que la règle d'exclusion est respectée et qu'aucun élément à un ensemble défini récursivement, sauf s'il se trouve dans la collection initiale spécifiée dans l'étape de base ou s'il peut être généré en utilisant l'étape récursive une ou plusieurs fois. Plus tard, nous verrons comment utiliser un technique connue sous le nom d'induction structurale pour prouver les résultats sur des ensembles définis de manière récursive.

Les exemples 5, 6, 8 et 9 illustrent la définition récursive des ensembles. Dans chaque exemple, nous montrons ces éléments générés par les premières applications de l'étape récursive.

EXEMPLE 5 Considérons le sous-ensemble S de l'ensemble d'entiers défini récursivement par

BASE ÉTAPE: $3 \in S$.

RÉCURSIVE ÉTAPE: Si $x \in S$ et $y \in S$, alors $x + y \in S$.

Les nouveaux éléments trouvés en S sont 3 à l'étape de base, $3 + 3 = 6$ à la première application de l'étape récursive, $3 + 6 = 6 + 3 = 9$ et $6 + 6 = 12$ à la deuxième application du récursif étape, et ainsi de suite. Nous montrerons dans l'exemple 10 que S est l'ensemble de tous les multiples positifs de 3. ▲

Les définitions récursives jouent un rôle important dans l'étude des chaînes. (Voir le chapitre 13 pour une introduction à la théorie des langages formels, par exemple.) Rappelons à la section 2.4 qu'un chaîne sur un alphabet est une séquence finie de symboles de. On peut définir *, l'ensemble des chaînes sur, récursivement, comme le montre la définition 1.

DÉFINITION 1 L'ensemble * de *chaînes* sur l'alphabet est défini récursivement par

ÉTAPE DE BASE: $\lambda \in {}^*$ (où λ est la chaîne vide ne contenant aucun symbole).

ÉTAPE RÉCURSIVE: Si $w \in {}^*$ et $x \in$, puis $wx \in {}^*$.

GABRIEL LAMÉ (1795-1870) Gabriel Lamé entre à l'École polytechnique en 1813 et obtient son diplôme en 1817. Il poursuit ses études à l'École des Mines et obtient son diplôme en 1820.

En 1820, Lamé se rend en Russie, où il est nommé directeur des écoles des autoroutes et des transports portation à Saint-Pétersbourg. Non seulement il a enseigné, mais il a également planifié des routes et des ponts en Russie. Il retourné à Paris en 1832, où il a aidé à fonder une firme d'ingénierie. Cependant, il a rapidement quitté l'entreprise, acceptant titulaire de la chaire de physique de l'École polytechnique, qu'il conserva jusqu'en 1844. Tout en occupant ce poste, il fut actif en dehors du milieu universitaire en tant que consultant en ingénierie, servant d'ingénieur en chef des mines et participant à la construction de chemins de fer.

Lamé a contribué à des travaux originaux sur la théorie des nombres, les mathématiques appliquées et la thermodynamique. De son mieux-les travaux connus impliquent l'introduction de coordonnées curvilignes. Son travail sur la théorie des nombres comprend la démonstration du dernier théorème de Fermat pour $n = 7$, en plus de fournir la borne supérieure du nombre de divisions utilisées par l'algorithme euclidien donné dans ce texte.

De l'avis de Gauss, l'un des mathématiciens les plus importants de tous les temps, Lamé était le plus grand mathématicien français de Son temps. Cependant, les mathématiciens français le considéraient comme trop pratique, tandis que les scientifiques français le considéraient trop théorique.

L'étape de base de la définition récursive des chaînes indique que la chaîne vide appartient à *. L'étape récursive indique que de nouvelles chaînes sont produites en ajoutant un symbole de à la fin de cordes dans *. A chaque application de l'étape récursive, des chaînes contenant un symbole supplémentaire Sont générés.

EXEMPLE 6 Si $= \{0, 1\}$, les chaînes trouvées dans *, l'ensemble de toutes les chaînes de bits, estλ, spécifié pour être dans * à l'étape de base, 0 et 1 formés lors de la première application de l'étape récursive, 00, 01, 10, et 11 formés lors de la deuxième application de l'étape récursive, et ainsi de suite. ▲

Des définitions récursives peuvent être utilisées pour définir des opérations ou des fonctions sur les éléments de ensembles définis récursivement. Ceci est illustré dans la définition 2 de la concaténation de deux chaînes et l'exemple 7 concernant la longueur d'une chaîne.

DÉFINITION 2 Deux chaînes peuvent être combinées via l'opération de*concaténation* . Laisser être un ensemble de symboles et * l'ensemble de chaînes formé de symboles en. On peut définir la concaténation de deux chaînes, notées par ·, récursivement comme suit.

ÉTAPE DE BASE: Si $w \in {}^*$, alors $w \cdot \lambda = w$, où λ est la chaîne vide.

ÉTAPE RÉCURSIVE: Si $w_1 \in {}^*$ et $w_2 \in {}^*$ et $x \in$, alors $w_1 \cdot (w_2 x) = (w_1 \cdot w_2)\, x$.

La concaténation des chaînes w_1 et w_2 est souvent écrite comme $w_1 w_2$ plutôt que $w_1 \cdot w_2$. Par l'application répétée de la définition récursive, il s'ensuit que la concaténation de deux chaînes w_1 et w_2 sont constitués des symboles de w_1 suivis des symboles de w_2 . Par exemple, le la concaténation de $w_1 = abra$ et $w_2 = cadabra$ est $w_1 w_2 = abracadabra$.

EXEMPLE 7 **Longueur d'une chaîne** Donnez une définition récursive de $l(w)$, la longueur de la chaîne w .

Solution: La longueur d'une chaîne peut être définie récursivement par

$l(\lambda) = 0$;

$l(wx) = l(w) + 1$ si $w \in {}^*$ et $x \in$. ▲

Une autre utilisation importante des définitions récursives consiste à définir **des formules bien formées** de les types. Ceci est illustré dans les exemples 8 et 9.

EXEMPLE 8 **Formules bien formées dans la logique propositionnelle** Nous pouvons définir l'ensemble de for-mulae dans la logique propositionnelle impliquant **T, F,** les variables propositionnelles et les opérateurs de l'ensemble $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.

BASE STEP: **T** , **F** , et s , où s est une variable propositionnelle, sont des formules bien formées.

ÉTAPE RÉCURIVE: Si E et F sont des formules bien formées, alors $(\neg E)$, $(E \wedge F)$, $(E \vee F)$, $(E \rightarrow F)$ et $(E \leftrightarrow F)$ sont des formules bien formées.

Par exemple, par l'étape de base, nous savons que **T** , **F** , p et q sont des formules bien formées, où p et q sont des variables propositionnelles. A partir d'une application initiale de l'étape récursive, nous savons que $(p \vee q)$, $(p \rightarrow \mathbf{F})$, $(\mathbf{F} \rightarrow q)$ et $(q \wedge \mathbf{F})$ sont des formules bien formées. Une seconde-

La deuxième application de l'étape récursive montre que $((p \vee q) \rightarrow (q \wedge \mathbf{F}))$, $(q \vee (p \vee q))$, et $((p \rightarrow \mathbf{F}) \rightarrow \mathbf{T})$ sont des formules bien formées. Nous laissons au lecteur le soin de montrer que $p \neg \wedge q$, $pq \wedge$, et $\neg \wedge pq$ ne sont *pas* des formules bien formées, en montrant qu'aucune ne peut être obtenue en utilisant l'étape de base et une ou plusieurs applications de l'étape récursive. ▲

Épisode 372

EXEMPLE 9 Formules d'opérateurs et d'opérandes bien formées On peut définir l'ensemble des ensembles bien formés formules composées de variables, de chiffres et d'opérateurs de l'ensemble $\{+, -, *, /, \uparrow\}$ (où $*$ dénote la multiplication et $\uparrow$ dénote l'exponentiation) récursivement.

ÉTAPE DE BASE: x est une formule bien formée si x est un chiffre ou une variable.

ÉTAPE RÉCURIVE: Si F et G sont des formules bien formées, alors $(F + G)$, $(F - G)$, $(F * G)$, (F / G) et $(F \uparrow G)$ sont des formules bien formées.

Par exemple, à l'étape de base, nous voyons que x , y , 0 et 3 sont des formules bien formées (comme toute variable ou chiffre). Formules bien formées générées en appliquant l'étape récursive une fois inclure $(x + 3)$, $(3 + y)$, $(x - y)$, $(3 - 0)$, $(x * 3)$, $(3 * y)$, $(3 / 0)$, (x / y) , $(3 \uparrow x)$ et $(0 \uparrow 3)$. L'application de l'étape récursive deux fois montre que des formules telles que $((x + 3) + 3)$ et $(x - (3 * y))$ sont des formules bien formées. [Notez que $(3 / 0)$ est une formule bien formée parce que nous sommes préoccupés par seulement avec la syntaxe importe ici.] Nous laissons au lecteur le soin de montrer que chacune des formules x 3 +, $y * + x$, et $* x / y$ n'est *pas* une formule bien formée en montrant qu'aucun d'eux ne peut être obtenu à partir de l'étape de base et d'une ou plusieurs applications de l'étape récursive. ▲

Nous étudierons les arbres en détail au chapitre 11. Un arbre est un type spécial de graphique; un graphique est composé de sommets et d'arêtes reliant certaines paires de sommets. Nous étudierons les graphiques dans Chapitre 10. Nous allons les présenter brièvement ici pour illustrer comment ils peuvent être définis de manière récursive.

DÉFINITION 3 L'ensemble d' *arbres enracinés,* où un arbre enraciné se compose d'un ensemble de sommets contenant une distinction sommet verte appelé la *racine,* et les bords reliant ces sommets, peuvent être définis récursivement par ces étapes:

ÉTAPE DE BASE: Un seul sommet r est un arbre enraciné.

ÉTAPE RÉCURSIVE: Supposons que T_1 , T_2 , ..., T_n sont des arbres à racines disjointes avec des racines r_1 , r_2 , ..., r_n , respectivement. Ensuite, le graphique formé en commençant par une racine r , qui n'est pas dans l'un des arbres enracinés T_1 , T_2 , ..., T_n , et en ajoutant une arête de r à chacun des sommets r_1 , r_2 , ..., r_n , est également un arbre enraciné.

Dans la figure 2, nous illustrons certains des arbres enracinés formés à partir de l'étape de base et en appliquant l'étape récursive une fois et deux fois. Notez qu'une infinité d'arbres enracinés se forment à chaque application de la définition récursive.

Étape de base

Étape 1

Étape 2

... ...

FIGURE 2 Construire des arbres enracinés.

Étape de base 0

Étape 1

Étape 2

Étape 3

FIGURE 3 **Création d'arbres binaires étendus.**

Les arbres binaires sont un type spécial d'arbres enracinés. Nous fournirons des définitions récursives de deux types d'arbres binaires: les arbres binaires complets et les arbres binaires étendus. Dans l'étape récursive de la définition de chaque type d'arbre binaire, deux arbres binaires sont combinés pour former un nouvel arbre avec l'un de ces arbres désigné sous-arbre gauche et l'autre sous-arbre droit. En extension les arbres binaires, le sous-arbre gauche ou le sous-arbre droit peuvent être vides, mais dans les arbres binaires pleins ce n'est pas possible. Les arbres binaires sont l'un des types de structures les plus importants en informatique. Dans Chapitre 11, nous verrons comment ils peuvent être utilisés dans les algorithmes de recherche et de tri, dans les algorithmes pour compresser les données et dans de nombreuses autres applications. Nous définissons d'abord les arbres binaires étendus.

DÉFINITION 4 L'ensemble d' *arbres binaires étendus* peut être défini récursivement par ces étapes:

ÉTAPE DE BASE: L'ensemble vide est un arbre binaire étendu.

ÉTAPE RÉCURIVE: Si T_1 et T_2 sont des arbres binaires étendus disjoints, il existe un arbre binaire, noté $T_1 \cdot T_2$, composé d'une racine r avec des arêtes reliant le racine à chacune des racines du sous-arbre gauche T_1 et du sous-arbre droit T_2 lorsque ces arbres sont non vide.

La figure 3 montre comment les arbres binaires étendus sont construits en appliquant l'étape récursive à partir d'un à trois fois.

Nous montrons maintenant comment définir l'ensemble d'arbres binaires complets. Notez que la différence entre cette définition récursive et celle des arbres binaires étendus se situe entièrement dans l'étape de base.

Étape de base

Étape 1

Étape 2

FIGURE 4 Création d'arbres binaires complets.

DÉFINITION 5 L'ensemble d'arbres binaires complets peut être défini récursivement par ces étapes:

ÉTAPE DE BASE: Il existe un arbre binaire complet composé uniquement d'un seul sommet r .

ÉTAPE RÉCURSIVE: Si T_1 et T_2 sont des arbres binaires complets disjoints, il y a un arbre binaire complet, notée $T_1 \cdot T_2$, consistant en une racine r avec des bords reliant la racine à chacun des les racines du sous-arbre gauche T_1 et du sous-arbre droit T_2 .

La figure 4 montre comment les arbres binaires complets sont construits en appliquant les étapes récursives un et deux fois.

Induction structurelle

Pour prouver les résultats sur des ensembles définis récursivement, nous utilisons généralement une certaine forme de mathématiques induction. L'exemple 10 illustre la connexion entre des ensembles définis récursivement et des induction matique.

EXEMPLE 10 Montrer que l'ensemble S défini dans l'exemple 5 en spécifiant que $3 \in S$ et que si $x \in S$ et $y \in S$, alors $x + y \in S$, est l'ensemble de tous les entiers positifs qui sont des multiples de 3.

Solution: Soit A l'ensemble de tous les entiers positifs divisibles par 3. Pour prouver que $A = S$, il faut montrent que A est un sous -ensemble de S et S est un sous -ensemble de A . Pour prouver que A est un sous-ensemble de S , nous doit montrer que chaque divisibles entier positif par 3 est en S . Nous utiliserons l'induction mathématique pour le prouver.

Laissez - $P(n)$ soit l'affirmation selon laquelle $3n$ appartient à S . L'étape de base tient parce que par le premier partie de la définition récursive de S , $3 \cdot 1 = 3$ est S . Pour établir l'étape inductive, supposez que $P(k)$ est vrai, à savoir que $3k$ se trouve dans S . Parce que $3k$ est en S et parce que 3 est en S , il suit à partir de la deuxième partie de la définition récursive de S que $3k + 3 = 3(k + 1)$ est également en S .

Pour prouver que S est un sous -ensemble de A , nous utilisons la définition récursive de S . Tout d'abord, l'étape de base de la définition précise que 3 est en S . Parce que $3 = 3 \cdot 1$, tous les éléments spécifiés pour être dans S dans cette étape est divisible par 3 et sont donc en A . Pour finir la preuve, il faut montrer que tous nombres entiers S générés en utilisant la seconde partie de la définition récursive sont en A . Cela consiste de montrer que $x + y$ est dans A chaque fois que x et y sont des éléments de S également supposé être dans A . Maintenant si x et y sont tous deux dans A , il s'ensuit que $3 \mid x$ et $3 \mid y$. Par la partie (i) du théorème 1 de la section 4.1, il s'ensuit que $3 \mid x + y$, complétant la preuve. ▲

Dans l'exemple 10, nous avons utilisé l'induction mathématique sur l'ensemble des entiers positifs et un définition récursive pour prouver un résultat sur un ensemble défini récursivement. Cependant, au lieu d'utiliser induction mathématique directement pour prouver les résultats sur des ensembles définis récursivement, nous pouvons utiliser un plus forme d'induction commode connue sous le nom d'**induction structurelle** . Une preuve par induction structurelle se compose de deux parties. Ces pièces sont

ÉTAPE DE BASE: montrer que le résultat est valable pour tous les éléments spécifiés dans l'étape de base du définition récursive pour être dans l'ensemble.

ÉTAPE RÉCURSIVE: Montrez que si l'énoncé est vrai pour chacun des éléments utilisés pour construire nouveaux éléments dans l'étape récursive de la définition, le résultat est valable pour ces nouveaux éléments.

La validité de l'induction structurelle découle du principe de l'induction mathématique pour les entiers non négatifs. Pour voir cela, laissez $P(n)$ déclarer que la revendication est vraie pour tous les éléments de l'ensemble qui sont générés par n ou moins applications des règles dans l'étape récursive de une définition récursive. Nous aurons établi que le principe de l'induction mathématique implique le principe de l'induction structurelle si nous pouvons montrer que $P(n)$ est vrai chaque fois que n est un entier positif. Dans l'étape de base d'une preuve par induction structurelle, nous montrons que $P(0)$ est vrai. Autrement dit, nous montrons que le résultat est vrai de tous les éléments spécifiés pour être dans l'ensemble dans la base étape de la définition. Une conséquence de l'étape récursive est que si nous supposons que $P(k)$ est vrai, il s'ensuit que $P(k+1)$ est vrai. Lorsque nous avons terminé une preuve par induction structurelle, nous avons montré que $P(0)$ est vrai et que $P(k)$ implique $P(k+1)$. Par induction mathématique, il s'ensuit que $P(n)$ est vrai pour tous les entiers non négatifs n. Cela montre également que le résultat est vrai pour tous les éléments générés par la définition récursive, et montre que l'induction structurelle est un technique de preuve valide.

EXEMPLES DE PREUVES UTILISANT UNE INDUCTION STRUCTURELLE L'induction structurelle peut être utilisé pour prouver que tous les membres d'un ensemble construit récursivement ont une propriété particulière. Nous allons illustrer cette idée en utilisant l'induction structurelle pour prouver les résultats sur une bonne formation formules, chaînes et arbres binaires. Pour chaque preuve, nous devons effectuer la base appropriée étape et l'étape récursive appropriée. Par exemple, pour utiliser une induction structurelle pour prouver un résultat sur l'ensemble des formules bien formées définies dans l'exemple 8, où l'on précise que **T** , **F** , et chaque variable propositionnelle s sont des formules bien formées et où nous spécifions que si E et F sont des formules bien formées, puis $(\neg E)$, $(E \wedge F)$, $(E \vee F)$, $(E \rightarrow F)$ et $(E \leftrightarrow F)$ sont des formules bien formées, nous devons compléter cette étape de base et cette étape récursive.

ÉTAPE DE BASE: Montrer que le résultat est vrai pour **T** , **F** et s chaque fois que s est une variable propositionnelle.

ÉTAPE RÉCURSIVE: Montrez que si le résultat est vrai pour les propositions composées p et q, il est également vrai pour $(\neg p)$, $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$ et $(p \leftrightarrow q)$.

L'exemple 11 illustre comment nous pouvons prouver les résultats de formules bien formées à l'aide de structures induction.

EXEMPLE 11 Montrer que chaque formule bien formée pour des propositions de composés, telle que définie dans l'exemple 8, contient un nombre égal de parenthèses gauche et droite.

Solution:

ÉTAPE DE BASE: Chacune des formules **T** , **F** et s ne contient pas de parenthèses, donc elles contiennent clairement un nombre égal de parenthèses gauche et droite.

ÉTAPE RÉCURIVE: Supposons que p et q sont des formules bien formées contenant chacune un égal nombre de parenthèses gauche et droite. Autrement dit, si l_p et l_q sont le nombre de parenthèses gauches en p et q, respectivement, et r_p et r_q sont le nombre de parenthèses droites en p et q, respectivement, alors $l_p = r_p$ et $l_q = r_q$. Pour terminer l'étape inductive, nous devons montrer que chacun des

$(\neg p)$, $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$ et $(p \leftrightarrow q)$ contiennent également un nombre égal de gauche et de droite parenthèses. Le nombre de parenthèses gauches dans la première de ces propositions composées est égal à $l_p + 1$ et dans chacune des autres propositions composées est égal à $l_p + l_q + 1$. De même, le nombre des parenthèses droites dans la première de ces propositions composées est égal à $r_p + 1$ et dans chacune des d'autres propositions composées sont égales à $r_p + r_q + 1$. Puisque $l_p = r_p$ et $l_q = r_q$, il s'ensuit que chacune de ces expressions composées contient le même nombre de parenthèses gauche et droite. Ceci complète la preuve par induction structurelle. ▲

Supposons que $P(w)$ est une fonction propositionnelle sur l'ensemble des chaînes $w \in {}^*$. Pour utiliser structurel induction pour prouver que $P(w)$ est valable pour toutes les chaînes $w \in$ nous devons terminer une étape de base et une étape récursive. Ces étapes sont les suivantes:

ÉTAPE DE BASE: Montrez que $P(\lambda)$ est vrai.

ÉTAPE RÉCURRENTE: Supposons que $P(w)$ est vrai, où $w \in {}^*$. Montrer que si $x \in$, alors $P(wx)$ doit également être vrai.

L'exemple 12 illustre comment l'induction structurelle peut être utilisée dans les preuves de chaînes.

EXEMPLE 12 Utiliser l'induction structurelle pour prouver que $l(xy) = l(x) + l(y)$, où x et y appartiennent à *, l'ensemble de chaînes sur l'alphabet.

Solution: Nous baserons notre preuve sur la définition récursive de l'ensemble * donnée dans la définition 1 et la définition de la longueur d'une chaîne dans l'exemple 7, qui spécifie que $l(\lambda) = 0$ et $l(wx) = l(w) + 1$ lorsque $w \in {}^*$ et $x \in$. Soit $P(y)$ la déclaration que $l(xy) = l(x) + l(y)$ chaque fois que x appartient *.

ÉTAPE DE BASE: Pour terminer l'étape de base, nous devons montrer que $P(\lambda)$ est vrai. Autrement dit, nous devons montrer que $l(x\lambda) = l(x) + l(\lambda)$ pour tout $x \in {}^*$. Parce que $l(x\lambda) = l(x) = l(x) + 0 = l(x) + l(\lambda)$ pour chaque chaîne x, il s'ensuit que $P(\lambda)$ est vrai.

ÉTAPE RÉCURIVE: Pour terminer l'étape inductive, nous supposons que $P(y)$ est vrai et montrer que cela implique que $P(ya)$ est vrai chaque fois *que* $\in$. Ce que nous devons montrer, c'est que $l(xya) = l(x) + l(ya)$ pour chaque $a \in$. Pour le montrer, notons que par la définition récursive de $l(w)$ (donné dans l'exemple 7), nous avons $l(xya) = l(xy) + 1$ et $l(ya) = l(y) + 1$. Et, par l'inductif hypothèse, $l(xy) = l(x) + l(y)$. Nous concluons que $l(xya) = l(x) + l(y) + 1 = l(x) + l(ya)$. ▲

Nous pouvons prouver des résultats sur des arbres ou des classes spéciales d'arbres en utilisant l'induction structurelle. Pour par exemple, pour prouver un résultat sur les arbres binaires complets en utilisant l'induction structurelle, nous devons compléter cette étape de base et cette étape récursive.

ÉTAPE DE BASE: Montrez que le résultat est vrai pour l'arbre composé d'un seul sommet.

ÉTAPE RÉCURIVE: Montrer que si le résultat est vrai pour les arbres T_1 et T_2, alors c'est vrai pour arbre $T_1 \cdot T_2$ composé d'une racine r, qui a T_1 comme sous-arbre gauche et T_2 comme sous-arbre droit.

Avant de fournir un exemple montrant comment l'induction structurelle peut être utilisée pour prouver résultat sur les arbres binaires complets, nous avons besoin de quelques définitions. Nous définirons récursivement la hauteur $h(T)$ et le nombre de sommets $n(T)$ d'un arbre binaire complet T. On commence par définir la hauteur d'un arbre binaire complet.

DÉFINITION 6 Nous définissons la hauteur $h(T)$ d'un arbre binaire complet T récursivement.

ÉTAPE DE BASE: La hauteur de l'arbre binaire complet T composé uniquement d'une racine r est $h(T) = 0$.

ÉTAPE RÉCURIVE: Si T_1 et T_2 sont des arbres binaires complets, alors l'arbre binaire complet $T = T_1 \cdot T_2$ a une hauteur $h(T) = 1 + \max(h(T_1), h(T_2))$.

Si nous laissons $n(T)$ le nombre de sommets dans un arbre binaire complet, nous observons que $n(T)$ satisfait la formule récursive suivante:

ÉTAPE DE BASE: Le nombre de sommets $n(T)$ de l'arbre binaire complet T constitué uniquement d'une racine r est $n(T) = 1$.

ÉTAPE RÉCURIVE: Si T_1 et T_2 sont des arbres binaires pleins, alors le nombre de sommets du plein arbre binaire $T = T_1 \cdot T_2$ est $n(T) = 1 + n(T_1) + n(T_2)$.

Nous montrons maintenant comment l'induction structurelle peut être utilisée pour prouver un résultat sur des arbres binaires complets.

THÉORÈME 2 Si T est un arbre binaire complet T, alors $n(T) \leq 2^{h(T)+1} - 1$.

Preuve: Nous prouvons cette inégalité par induction structurelle.

ÉTAPE DE BASE: Pour l'arbre binaire complet constitué uniquement de la racine r, le résultat est vrai car $n(T) = 1$ et $h(T) = 0$, de sorte que $n(T) = 1 \leq 2^{0+1} - 1 = 1$.

ÉTAPE RÉCURIVE: Pour l'hypothèse inductive, nous supposons que $n(T_1) \leq 2^{h(T_1)+1} - 1$ et $n(T_2) \leq 2^{h(T_2)+1} - 1$ lorsque T_1 et T_2 sont des arbres binaires complets. Par les formules récursives pour $n(T)$ et $h(T)$ nous avons $n(T) = 1 + n(T_1) + n(T_2)$ et $h(T) = 1 + \max(h(T_1), h(T_2))$.

Nous constatons que

$$
\begin{aligned}
n(T) &= 1 + n(T_1) + n(T_2) && \text{par la formule récursive pour } n(T) \\
&\leq 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1) && \text{par l'hypothèse inductive} \\
&\leq 2 \cdot \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1 && \text{parce que la somme de deux termes est au plus 2 fois le plus grand} \\
&= 2 \cdot 2^{\max(h(T_1), h(T_2))+1} - 1 && \text{car } \max(2^x, 2^y) = 2^{\max(x, y)} \\
&= 2 \cdot 2^{h(T)} - 1 && \text{par la définition récursive de } h(T) \\
&= 2^{h(T)+1} - 1.
\end{aligned}
$$

Ceci termine l'étape récursive.

Induction généralisée

Nous pouvons étendre l'induction mathématique pour prouver les résultats sur d'autres ensembles qui ont le bien-ordre de la propriété en plus de l'ensemble des entiers. Bien que nous aborderons ce concept en détail dans À la section 9.6, nous donnons ici un exemple pour illustrer l'utilité d'une telle approche.

A titre d'exemple, notons que nous pouvons définir un ordre sur $\mathbf{N} \times \mathbf{N}$, les paires ordonnées de non entiers négatifs, en spécifiant que (x_1, y_1) est inférieur ou égal à (x_2, y_2) si soit $x_1 < x_2$, ou $x_1 = x_2$ et $y_1 < y_2$; c'est ce qu'on appelle l' **ordre lexicographique** . L'ensemble $\mathbf{N} \times \mathbf{N}$ avec ce l'ordre a la propriété que chaque sous-ensemble de $\mathbf{N} \times \mathbf{N}$ a un moindre élément (voir Exercice 53 dans la section 9.6). Cela implique que nous pouvons définir récursivement les termes $a_{m,n}$, avec $m \in \mathbf{N}$ et $n \in \mathbf{N}$, et prouver les résultats à leur sujet en utilisant une variante d'induction mathématique, comme illustré dans Exemple 13.

EXEMPLE 13 Supposons qu'un $a_{,n}$ est défini récursivement pour $(m, n) \in \mathbf{N} \times \mathbf{N}$ par $un_{0,0} = 0$ et

$$
a_{m,n} = \begin{cases} a_{m-1,n} + 1 & \text{si } n = 0 \text{ et } m > 0 \\ a_{m,n-1} + n & \text{si } n > 0. \end{cases}
$$

Montrer que $a_{m,n} = m + n(n+1)/2$ pour tous $(m, n) \in \mathbf{N} \times \mathbf{N}$, c'est-à-dire pour toutes les paires de non négatives entiers.

Solution: Nous pouvons prouver que $un_{m,n} = m + n(n+1)/2$ en utilisant une version généralisée de mathématique induction. L'étape de base nécessite que nous montrions que cette formule est valide lorsque $(m, n) = (0, 0)$. L'étape d'induction nécessite que nous montrions que si la formule est vraie pour toutes les paires plus petites que (m, n) dans l'ordre lexicographique de $\mathbf{N} \times \mathbf{N}$, alors il en va de même pour (m, n).

ÉTAPE DE BASE: Soit $(m, n) = (0, 0)$. Ensuite, par le cas de base de la définition récursive d'$un_{m,n}$ nous avons $un_{0,0} = 0$. De plus, lorsque $m = n = 0$, $m + n(n+1)/2 = 0 + (0 \cdot 1)/2 = 0$. Ce termine l'étape de base.

ÉTAPE INDUCTIVE: Supposons que $a_{m,n} = m + n(n+1)/2$ chaque fois que (m, n) est inférieur de (m, n) dans l'ordre lexicographique de $\mathbf{N} \times \mathbf{N}$. Par la définition récursive, si $n = 0$, alors $a_{m,n} = a_{m-1,n} + 1$. Parce que $(m-1, n)$ est plus petit que (m, n), l'hypothèse inductive esis nous dit que $a_{m-1,n} = m - 1 + n(n+1)/2$, de sorte que $a_{m,n} = m - 1 + n(n+1)/2 + 1 = m + n(n+1)/2$, nous donnant l'égalité souhaitée. Supposons maintenant que $n > 0$, donc $a_{m,n} = a_{m,n-1} + n$.

Parce que $(m, n-1)$ est plus petit que (m, n), l'hypothèse inductive nous dit que $a_{m,n-1} = m + (n-1)n/2$, donc $a_{m,n} = m + (n-1)n/2 + n = m + (n^2 - n + 2n)/2 = m + n(n+1)/2$.

Ceci termine l'étape inductive. ▲

Comme mentionné, nous justifierons cette technique de preuve dans la section 9.6.

Des exercices

1. Trouvez $f(1)$, $f(2)$, $f(3)$ et $f(4)$ si $f(n)$ est défini récurrent par $f(0) = 1$ et pour $n = 0, 1, 2, \ldots$

a) $f(n+1) = f(n) + 2$.

b) $f(n+1) = 3f(n)$.

5. Déterminez si chacune de ces définitions proposées est une définition récursive valide d'une fonction f de l'ensemble des entiers non négatifs à l'ensemble des entiers. Si f va bien défini, trouver une formule pour $f(n)$ lorsque n est un négatif

c) $f(n+1) = 2^{f(n)}$.
d) $f(n+1) = f(n)^2 + f(n) + 1$.

2. Trouvez $f(1)$, $f(2)$, $f(3)$, $f(4)$ et $f(5)$ si $f(n)$ est défini récursivement par $f(0) = 3$ et pour $n = 0, 1, 2, \ldots$

a) $f(n+1) = -2f(n)$.
b) $f(n+1) = 3f(n) + 7$.
c) $f(n+1) = f(n)^2 - 2f(n) - 2$.
d) $f(n+1) = 3^{f(n)/3}$.

3. Trouvez $f(2)$, $f(3)$, $f(4)$ et $f(5)$ si f est défini récurrent par $f(0) = -1, f(1) = 2$, et pour $n = 1, 2, \ldots$

a) $f(n+1) = f(n) + 3f(n-1)$.
b) $f(n+1) = f(n)^2 f(n-1)$.
c) $f(n+1) = 3f(n)^2 - 4f(n-1)^2$.
d) $f(n+1) = f(n-1) / f(n)$.

4. Trouvez $f(2)$, $f(3)$, $f(4)$ et $f(5)$ si f est défini récurrent par $f(0) = f(1) = 1$ et pour $n = 1, 2, \ldots$

a) $f(n+1) = f(n) - f(n-1)$.
b) $f(n+1) = f(n) f(n-1)$.
c) $f(n+1) = f(n)^2 + f(n-1)^3$.
d) $f(n+1) = f(n) / f(n-1)$.

entier et prouver que votre formule est valide.

a) $f(0) = 0, f(n) = 2f(n-2)$ pour $n \geq 1$
b) $f(0) = 1, f(n) = f(n-1) - 1$ pour $n \geq 1$
c) $f(0) = 2, f(1) = 3, f(n) = f(n-1) - 1$ pour $n \geq 2$
d) $f(0) = 1, f(1) = 2, f(n) = 2f(n-2)$ pour $n \geq 2$
e) $f(0) = 1, f(n) = 3f(n-1)$ si n est impair et $n \geq 1$ et $f(n) = 9f(n-2)$ si n est pair et $n \geq 2$

6. Déterminez si chacune de ces définitions proposées est une définition récursive valide d'une fonction f de l'ensemble des entiers non négatifs à l'ensemble des entiers. Si f va bien défini, trouver une formule pour $f(n)$ lorsque n est un négatif entier et prouver que votre formule est valide.

a) $f(0) = 1, f(n) = -f(n-1)$ pour $n \geq 1$
b) $f(0) = 1, f(1) = 0, f(2) = 2, f(n) = 2f(n-3)$ pour $n \geq 3$
c) $f(0) = 0, f(1) = 1, f(n) = 2f(n+1)$ pour $n \geq 2$
d) $f(0) = 0, f(1) = 1, f(n) = 2f(n-1)$ pour $n \geq 1$
e) $f(0) = 2, f(n) = f(n-1)$ si n est impair et $n \geq 1$ et $f(n) = 2f(n-2)$ si $n \geq 2$

7. Donnez une définition récursive de la séquence $\{a_n\}$, $n = 1, 2, 3, \ldots$ si

a) $a_n = 6n$. **b)** $a_n = 2n + 1$.
c) $a_n = 10^n$. **d)** $a_n = 5$.

8. Donnez une définition récursive de la séquence $\{a_n\}$, $n = 1, 2, 3, \ldots$ si

a) $a_n = 4n - 2$. **b)** $a_n = 1 + (-1)^n$.
c) $a_n = n(n+1)$. **d)** $a_n = n^2$.

9. Soit F la fonction telle que $F(n)$ est la somme des premiers n entiers positifs. Donnez une définition récursive de $F(n)$.

10. Donnez une définition récursive de $S_m(n)$, la somme des ger m et l'entier non négatif n .

11. Donner une définition récursive de $P_m(n)$, le produit de la l'entier m et l'entier non négatif n .

Dans les exercices 12 à 19, f_n est le n ème nombre de Fibonacci.

12. Prouvez que $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$ lorsque n est un entier positif.

13. Montrer que $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$ lorsque n est un pos- entier itif.

∗ **14.** Montrer que $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ quand n est positif entier.

∗ **15.** Montrer que $f_0 f_1 + f_1 f_2 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2$ quand n est un entier positif.

∗ **16.** Spectacle cette $f_0 - f_1 + f_2 - \cdots - f_{2n-1} + f_{2n} = f_{2n-1} - 1$ lorsque n est un entier positif.

17. Déterminer le nombre de divisions utilisées par les euclidiens algorithme pour trouver le plus grand diviseur commun du Fi- nombres bonacci f_n et f_{n+1} , où n est un négatif entier. Vérifiez votre réponse en utilisant l'induction mathématique.

18. Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ \text{dix} \end{bmatrix}.$$

Montre CA

$$\mathbf{UNE} \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$$

lorsque n est un entier positif.

19. En prenant des déterminants des deux côtés de l'équation Exercice 18, prouver l'identité donnée dans l'exercice 14. (Réf. appeler que le déterminant de la matrice $\begin{vmatrix} un\ B \\ CD \end{vmatrix}$ C'est $ad - bc$.)

∗ **20.** Donner une définition récursive des fonctions max et min pour que max $(a_1, a_2, \ldots, a_n)$ et min $(a_1, a_2, \ldots, a_n)$ sont le maximum et le minimum des n nombres $a_1, a_2, \ldots, a_n$, respectivement.

∗ **21.** Soit $a_1, a_2, \ldots, a_n$ et $b_1, b_2, \ldots, b_n$ des nombres réels.

Utilisez les définitions récursives que vous avez données dans l'exercice 20 pour le prouver.

a) max $(-a_1, -a_2, \ldots, -a_n) = -$min $(a_1, a_2, \ldots, a_n)$

23. Donner une définition récursive de l'ensemble des entiers positifs qui sont des multiples de 5.

24. Donnez une définition récursive de

a) l'ensemble d'entiers positifs impairs.
b) l'ensemble des puissances entières positives de 3.
c) l'ensemble des polynômes à coefficients entiers.

25. Donnez une définition récursive de

a) l'ensemble des entiers pairs.
b) l'ensemble des entiers positifs congruents à 2 modulo 3.
c) l'ensemble d'entiers positifs non divisible par 5.

26. Soit S le sous-ensemble de l'ensemble des paires ordonnées d'entiers défini récursivement par

L' étape de la base: $(0, 0) \in S$.

Étape récursive: Si $(a, b) \in S$, alors $(a+2, b+3) \in S$ et $(a+3, b+2) \in S$.

a) Énumérer les éléments de S produits par les cinq premières applications de la définition récursive.
b) Utiliser une forte induction sur le nombre d'applications de l'étape récursive de la définition pour montrer que $5 \mid a + b$ quand $(a, b) \in S$.
c) Utiliser l'induction structurelle pour montrer que $5 \mid a + b$ quand $(a, b) \in S$.

27. Soit S le sous-ensemble de l'ensemble des paires ordonnées d'entiers défini récursivement par

L' étape de la base: $(0, 0) \in S$.

Étape récursive: Si $(a, b) \in S$, alors $(a, b+1) \in S$, $(a+1, b+1) \in S$, et $(a+2, b+1) \in S$.

a) Énumérer les éléments de S produits par les quatre premières applications de la définition récursive.
b) Utiliser une forte induction sur le nombre d'applications de l'étape récursive de la définition pour montrer que $a \leq 2b$ chaque fois que $(a, b) \in S$.
c) Utiliser l'induction structurelle pour montrer que $a \leq 2b$ quand- jamais $(a, b) \in S$.

28. Donnez une définition récursive de chacun de ces ensembles d'ordres paires d'entiers positifs. [*Astuce:* Tracer les points dans l'ensemble dans l'avion et recherchez les lignes contenant des points dans le ensemble.]

a) $S = \{(a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, et $a + b$ est impair$\}$
b) $S = \{(a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, et $un \mid b\}$
c) $S = \{(a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, Et $3 \mid a + b\}$

29. Donnez une définition récursive de chacun de ces ensembles d'or- paires dérivées d'entiers positifs. Utiliser l'induction structurelle pour prouver que la définition récursive que vous avez trouvée est correcte. [*Astuce:* pour trouver une définition récursive, tracez les points mis dans le plan et chercher des motifs.]

a) $S = \{(a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, et $a + b$ est pair$\}$

b) $\max(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \leq \max(a_1, a_2, \ldots, a_n) + \max(b_1, b_2, \ldots, b_n)$

c) $\min(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \geq \min(a_1, a_2, \ldots, a_n) + \min(b_1, b_2, \ldots, b_n)$

22. Montrer que l'ensemble S défini par $1 \in S$ et $s + t \in S$ quand-toujours $s \in S$ et $t \in S$ est l'ensemble des entiers positifs.

b) $S = \{ (a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, et a ou b est impair$\}$

c) $S = \{ (a, b) \mid a \in \mathbf{Z}^+, b \in \mathbf{Z}^+$, $a + b$ est impair et $3 \mid b \}$

30. Prouver que dans une chaîne de bits, la chaîne 01 apparaît au plus un plus de temps que la chaîne 10.

31. Définissez des formules bien formées d'ensembles, des variables des ensembles et des opérateurs de { , ∪ , ∩ , -}.

Épisode 380

32. a) donner une définition récursive de la fonction *les (s)* , qui compte le nombre de uns dans une chaîne de bits s .

b) Utiliser l'induction structurelle pour prouver que *ceux (st)* = *un (s) + un (t)* .

33. a) Donner une définition récursive de la fonction $m(s)$, qui est égal au plus petit chiffre d'une chaîne non vide de chiffres imaux.

b) Utiliser l'induction structurelle pour prouver que $m(st) = \min(m(s), m(t))$.

L' **inversion** d'une chaîne est la chaîne constituée des symboles de la chaîne dans l'ordre inverse. L'inversion de la chaîne w est dénoté par w^R.

34. Trouvez l'inversion des chaînes de bits suivantes.

a) 0101 **b)** 1 1011 **c)** 1000 1001 0111

35. Donnez une définition récursive de l'inversion d'une chaîne. [*Astuce:* définissez d'abord l'inversion de la chaîne vide. alors écrire une chaîne w de longueur $n + 1$ comme xy , où x est une chaîne de longueur n , et exprime l'inversion de w en termes de x^R et y .]

∗ **36.** Utiliser l'induction structurelle pour prouver que $(w_1 w_2)^R = w_2^R w_1^R$.

37. Donner une définition récursive de w^i, où w est une chaîne et i est un entier non négatif. (Ici w^i représente le caténation de i copies de la chaîne w .)

∗ **38.** Donner une définition récursive de l'ensemble des chaînes de bits qui sont palindromes.

39. Quand une chaîne appartient-elle à l'ensemble A de chaînes de bits condamné à une amende récursive

$\lambda \in A$

$0x1 \in A$ si $x \in A$,

où λ est la chaîne vide?

∗ **40.** Définissez récursivement l'ensemble de chaînes de bits qui ont plus des zéros que des uns.

41. Utilisez l'exercice 37 et l'induction mathématique pour montrer que $l(w^i) = i \cdot l(w)$, où w est une chaîne et i est un négatif entier.

∗ **42.** Montrer que $(w^R)^i = (w^i)^R$ chaque fois que w est une chaîne et que i est un entier non négatif; c'est-à-dire, montrer que le i ème pouvoir de l'inversion d'une chaîne est l'inversion de la i ème puissance de la chaîne.

43. Utiliser l'induction structurelle pour montrer que $n(T) \geq 2h(T) + 1$, où T est un arbre binaire complet, $n(T)$ est égal au nombre de sommets de T , et $h(t)$ est la hauteur de T .

L'ensemble des feuilles et l'ensemble des sommets internes d'un binaire complet L'arbre peut être défini récursivement.

Étape de base: La racine r est une feuille de l'arbre binaire complet avec exactement un sommet r . Cet arbre n'a pas de sommets internes.

Étape récursive: L'ensemble des feuilles de l'arbre $T = T_1 \cdot T_2$ est l'union des jeux de feuilles de T_1 et de T_2 . L'inter-les sommets finaux de T sont la racine r de T et l'union des ensemble de sommets internes de T_1 et l'ensemble de sommets internes de T_2 .

44. Utiliser l'induction structurelle pour montrer que $l(T)$, le nombre de feuilles d'un arbre binaire complet T , est 1 de plus que $i(T)$, le nombre de sommets internes de T .

45. Utiliser l'induction généralisée comme cela a été fait dans l'exemple 13 pour montrent que si $un_{m,n}$ est défini récursivement par $un_{0,0} = 0$ et

$$a_{m,n} = \begin{cases} a_{m-1,n} + 1 & \text{si } n = 0 \text{ et } m > 0 \\ a_{m,n-1} + 1 & \text{si } n > 0, \end{cases}$$

puis $un_{m,n} = m + n$ pour tous les $(m, n) \in \mathbf{N} \times \mathbf{N}$.

46. Utiliser l'induction généralisée comme cela a été fait dans l'exemple 13 pour montrent que si $a_{m,n}$ est défini récursivement par $un_{1,1} = 5$ et

$$a_{m,n} = \begin{cases} a_{m-1,n} + 2 & \text{si } n = 1 \text{ et } m > 1 \\ a_{m,n-1} + 2 & \text{si } n > 1, \end{cases}$$

alors $a_{m,n} = 2(m + n) + 1$ pour tout $(m, n) \in \mathbf{Z}^+ \times \mathbf{Z}^+$.

∗ **47.** Une **partition** d'un entier positif n est un moyen d'écrire n comme une somme d'entiers positifs où l'ordre des termes dans la somme n'a pas d'importance. Par exemple, $7 = 3 + 2 + 1 + 1$ est une partition de 7. Soit P_m égal au nombre de différents partitions de m , et soit $P_{m,n}$ le nombre de différents façons d'exprimer m comme la somme des entiers positifs non dépassant n .

a) Montrer que $P_{m,m} = P_m$.

b) Montrer que la définition récursive suivante pour $P_{m,n}$ est correct:

$$P_{m,n} = \begin{cases} 1 & \text{si } m = 1 \\ 1 & \text{si } n = 1 \\ P_{m,m} & \text{si } m < n \\ 1 + P_{m,m-1} & \text{si } m = n > 1 \\ P_{m,n-1} + P_{m-n,n} & \text{si } m > n > 1. \end{cases}$$

c) Trouvez le nombre de partitions de 5 et de 6 en utilisant ce définition récursive.

Considérons une définition inductive d'une version d' **Ackermann fonction** . Cette fonction a été nommée d'après Wilhelm Ackermann, un mathématicien allemand qui était un étudiant de la grande mathématique l'ématicien David Hilbert. La fonction d'Ackermann joue un rôle rôle important dans la théorie des fonctions récursives et dans l'étude de la complexité de certains algorithmes impliquant des unions d'ensemble. (Il existe plusieurs variantes de cette fonction. Toutes sont appelé la fonction d'Ackermann et ont même des propriétés similaires bien que leurs valeurs ne soient pas toujours d'accord.)

$$A(m, n) = \begin{cases} 2n & \text{si } m = 0 \\ 0 & \text{si } m \geq 1 \text{ et } n = 0 \\ 2 & \text{si } m \geq 1 \text{ et } n = 1 \\ A(m-1, A(m, n-1)) & \text{si } m \geq 1 \text{ et } n \geq 2 \end{cases}$$

Les exercices 48 à 55 impliquent cette version des fonctions d'Ackermann. tion.

48. Trouvez ces valeurs de la fonction d'Ackermann.

a) $A(1, 0)$ **b)** $A(0, 1)$

c) $A(1, 1)$ **d)** $A(2, 2)$

49. Montrer que $A(m, 2) = 4$ chaque fois que $m \geq 1$.

50. Montrer que $A(1, n) = 2^n$ chaque fois que $n \geq 1$.

51. Trouvez ces valeurs de la fonction d'Ackermann.

a) $A(2, 3)$ * **b)** $A(3, 3)$

∗ **52.** Trouvez $A(3, 4)$.

** **53.** Démontrer que $A(m, n+1) > A(m, n)$ chaque fois que m et n sont entiers non négatifs.

* **54.** Démontrer que $A(m+1, n) \geq A(m, n)$ chaque fois que m et n sont entiers non négatifs.

55. Démontrer que $A(i, j) \geq j$ lorsque i et j sont non négatifs entiers.

56. Utiliser l'induction mathématique pour prouver qu'une fonction F défini en spécifiant $F(0)$ et une règle d'obtention $F(n+1)$ de $F(n)$ est bien défini.

57. Utiliser une forte induction pour prouver qu'une fonction F définie par spécifiant $F(0)$ et une règle pour obtenir $F(n+1)$ *à* partir de les valeurs $F(k)$ pour $k = 0, 1, 2, \ldots, n$ sont bien définies.

58. Montrer que chacune de ces définitions récursives proposées de une fonction sur l'ensemble des entiers positifs ne produit pas une fonction bien définie.

a) $F(n) = 1 + F(\lfloor n/2 \rfloor)$ pour $n \geq 1$ et $F(1) = 1$.
b) $F(n) = 1 + F(n-3)$ pour $n \geq 2$, $F(1) = 2$, et $F(2) = 3$.
c) $F(n) = 1 + F(n/2)$ pour $n \geq 2$, $F(1) = 1$, et $F(2) = 2$.
d) $F(n) = 1 + F(n/2)$ si n est pair et $n \geq 2$, $F(n) = 1 - F(n-1)$ si n est impair, et $F(1) = 1$.
e) $F(n) = 1 + F(n/2)$ si n est pair et $n \geq 2$, $F(n) = F(3n-1)$ si n est impair et $n \geq 3$, et $F(1) = 1$.

59. Montrer que chacune de ces définitions récursives proposées de une fonction sur l'ensemble des entiers positifs ne produit pas une fonction bien définie.

a) $F(n) = 1 + F(\lfloor (n+1)/2 \rfloor)$ pour $n \geq 1$ et $F(1) = 1$.
b) $F(n) = 1 + F(n-2)$ pour $n \geq 2$ et $F(1) = 0$.
c) $F(n) = 1 + F(n/3)$ pour $n \geq 3$, $F(1) = 1$, $F(2) = 2$, et $F(3) = 3$.
d) $F(n) = 1 + F(n/2)$ si n est pair et $n \geq 2$, $F(n) = 1 + F(n-2)$ si n est impair, et $F(1) = 1$.
e) $F(n) = 1 + F(F(n-1))$ si $n \geq 2$ et $F(1) = 2$.

Les exercices 60 à 62 traitent des itérations de la fonction logarithme. Soit $\log n$ le logarithme de n à la base 2, comme d'habitude. le journal des fonctions $^{(k)} n$ est défini récursivement par

$$\text{Journal}^{(k)} n = \begin{cases} n & \text{si } k = 0 \\ \log(\text{journal}^{(k-1)} n) & \text{si } \log^{(k-1)} n \text{ est défini et positif} \\ \text{indéfini} & \text{autrement.} \end{cases}$$

Le **logarithme itéré** est le journal des fonctions $^{*} n$ dont la valeur à n est le plus petit entier non négatif k tel que $\log^{(k)} n \leq 1$.

60. Trouvez ces valeurs.

a) se connecter $^{(2)}$ 16 — **b)** journal$^{(3)}$ 256
c) journal$^{(3)}$ 2^{65536} — **d)** journal$^{(4)}$ $2^{2^{65536}}$

61. Trouver la valeur de $\log^{*} n$ pour ces valeurs de n.

a) 2 — **b)** 4 — **c)** 8 — **d)** 16
e) 256 — **f)** 65536 — **g)** 2^{2048}

62. Trouver le plus grand entier n tel que $\log^{*} n = 5$. Déterminez le nombre de chiffres décimaux dans ce nombre.

Les exercices 63 à 65 traitent des valeurs des fonctions itérées. Souper-pose que $f(n)$ est une fonction de l'ensemble des nombres réels, ou nombres réels positifs, ou un autre ensemble de nombres réels, pour l'ensemble des nombres réels tels que $f(n)$ est monotone rainage [c'est-à-dire, $f(n) < f(m)$ lorsque $n < m$) et $f(n) < n$ pour tout n dans le domaine de f.] La fonction $f^{(k)}(n)$ est définie récursivement par

$$f^{(k)}(n) = \begin{cases} n & \text{si } k = 0 \\ f(f^{(k-1)}(n)) & \text{si } k > 0. \end{cases}$$

De plus, soit c un nombre réel positif. L' **itéré fonction** f^{*}_{c} est le nombre d'itérations de f nécessaires pour réduire son argument à c ou moins, donc $f^{*}_{c}(n)$ est le plus petit non négatif entier k tel que $f^{k}(n) \leq c$.

63. Soit $f(n) = n - a$, où a est un entier positif. Trouver un formule pour $f^{(k)}(n)$. Quelle est la valeur de $f^{*}_{0}(n)$ lorsque n est un entier positif?

64. Soit $f(n) = n/2$. Trouvez une formule pour $f^{(k)}(n)$. Quel est le valeur de $f^{*}_{1}(n)$ lorsque n est un entier positif?

65. Soit $f(n) =$ n. Trouvez une formule pour $f^{(k)}(n)$. Quel est le valeur de $f^{*}_{2}(n)$ lorsque n est un entier positif?

Algorithmes récursifs

introduction

Parfois, nous pouvons réduire la solution à un problème avec un ensemble particulier de valeurs d'entrée au solution du même problème avec des valeurs d'entrée plus petites. Par exemple, le problème de trouver le plus grand diviseur commun de deux entiers positifs a et b, où $b > a$, peut être réduit pour trouver le plus grand diviseur commun d'une paire de plus petits entiers, à savoir, b **mod** a et a, car gcd $(b$ **mod** $a, a) =$ gcd (a, b). Lorsqu'une telle réduction peut être effectuée, la solution le problème d'origine peut être trouvé avec une séquence de réductions, jusqu'à ce que le problème ait été résolu réduit à un cas initial pour lequel la solution est connue. Par exemple, pour trouver le meilleur diviseur commun, la réduction se poursuit jusqu'à ce que le plus petit des deux nombres soit nul, car gcd $(a, 0) = a$ lorsque $a > 0$.

Voici un célèbre citation humoristique: «Pour comprendre la récursivité, vous doit d'abord comprendre récursivité. "

Nous verrons que les algorithmes qui réduisent successivement un problème au même problème avec des entrées plus petites sont utilisées pour résoudre une grande variété de problèmes.

DÉFINITION 1 Un algorithme est appelé *récursif* s'il résout un problème en le réduisant à une instance de la même problème avec une entrée plus petite.

Nous décrirons une variété d'algorithmes récursifs différents dans cette section.

EXEMPLE 1 Donner un algorithme récursif pour calculer n !, Où n est un entier non négatif.

Solution: Nous pouvons construire un algorithme récursif qui trouve n !, Où n est un entier non négatif, basé sur la définition récursive de n !, qui spécifie que $n ! = n \cdot (n - 1)$! quand n est positif entier, et que 0! = 1. Pour trouver n ! pour un entier particulier, on utilise l'étape récursive n fois, en remplaçant à chaque fois une valeur de la fonction factorielle par la valeur de la fonction factorielle à le plus petit entier suivant. À cette dernière étape, nous insérons la valeur de 0 !. L'algorithme récursif que nous get s'affiche sous la forme de l'algorithme 1.

Pour aider à comprendre le fonctionnement de cet algorithme, nous suivons les étapes utilisées par l'algorithme pour calculer 4 !. Tout d'abord, nous utilisons l'étape récursive pour écrire 4! = 4 · 3 !. On utilise ensuite le récursif étape à plusieurs reprises pour écrire 3! = 3 · 2 !, 2! = 2 · 1 !, et 1! = 1 · 0 !. Insertion de la valeur de 0!= 1, et en remontant les étapes, nous voyons que 1! = 1 · 1 = 1, 2! = 2 · 1! = 2, 3! = 3 · 2! = 3 · 2 = 6 et 4! = 4 · 3! = 4 · 6 = 24. ▲

ALGORITHME 1 Un algorithme récursif pour le calcul n !.

factorielle de **procédure** (n : entier non négatif)
si $n = 0$ **alors retourne** 1
sinon retourner $n \cdot$ *factoriel* $(n - 1)$
{la sortie est n !}

L'exemple 2 montre comment un algorithme récursif peut être construit pour évaluer une fonction à partir de son définition récursive.

EXEMPLE 2 Donner un algorithme récursif pour calculer *un* $_n$, où a est un nombre réel non nul et n est un entier non négatif.

Solution: on peut baser un algorithme récursif sur la définition récursive d'*un* $_n$. Cette définition indique que $a_{n+1} = a \cdot a_n$ pour $n > 0$ et la condition initiale $a_0 = 1$. Pour trouver *un* $_n$, successivement utilisez l'étape récursive pour réduire l'exposant jusqu'à ce qu'il devienne zéro. Nous donnons cette procédure en Algorithme 2. ▲

ALGORITHME 2 Un algorithme récursif pour le calcul d' ***un*** $_n$ **.**

puissance de **procédure** (a : nombre réel non nul, n : entier non négatif)
si $n = 0$ **alors retourne** 1
sinon retourne *une puissance* $\cdot$ *(a, n* - 1 *)*
{la sortie est *un*}$_n$

Ensuite, nous donnons un algorithme récursif pour trouver les plus grands diviseurs communs.

EXEMPLE 3 Donner un algorithme récursif pour calculer le plus grand diviseur commun de deux non négatifs les entiers a et b avec $a < b$.

Solution: On peut baser un algorithme récursif sur la réduction gcd(a, b) = gcd $(b$ **mod** $a, a)$ et la condition gcd $(0, b) = b$ lorsque $b > 0$. Cela produit la procédure dans l'algorithme 3, qui est une version récursive de l'algorithme euclidien.

Nous illustrons le fonctionnement de l'algorithme 3 avec une trace lorsque l'entrée est $a = 5$, $b = 8$. Avec cette entrée, l'algorithme utilise la clause "else" pour trouver que gcd $(5, 8)$ = gcd $(8$ **mod** $5, 5)$ = pgcd $(3, 5)$. Il utilise à nouveau cette clause pour trouver que gcd $(3, 5)$ = gcd $(5$ **mod** $3, 3)$ = gcd $(2, 3)$, puis pour obtenir gcd $(2, 3)$ = gcd $(3$ **mod** $2, 2)$ = gcd $(1, 2)$, puis pour obtenir gcd $(1, 2)$ = gcd $(2$ **mod** $1, 1)$ = pgcd $(0, 1)$. Enfin, pour trouver gcd $(0, 1)$, il utilise la première étape avec $a = 0$ pour trouver que gcd $(0, 1) = 1$. Par conséquent, l'algorithme trouve que gcd $(5, 8) = 1$. ▲

ALGORITHME 3 Un algorithme récursif pour calculer le pgcd (a, b) .

procédure *gcd* $(a, b$: entiers non négatifs avec $a < b)$
si $a = 0$ **alors retourne** b
sinon retourner *gcd* $(b$ **mod** $a, a)$
{la sortie est gcd (a, b) }

EXEMPLE 4 Concevoir un algorithme récursif pour calculer b^n **mod** m , où b , n et m sont des entiers avec $m \geq 2$, $n \geq 0$ et $1 \leq b < m$.

Solution: On peut baser un algorithme récursif sur le fait que

$$b^n \textbf{ mod } m = (b \cdot (b^{n-1} \textbf{ mod } m)) \textbf{ mod } m ,$$

qui suit par le corollaire 2 dans la section 4.1, et la condition initiale b^0 **mod** $m = 1$. Nous quittons cela comme exercice 12 pour le lecteur.

Cependant, nous pouvons concevoir un algorithme récursif beaucoup plus efficace basé sur l'observation cette

$$b^n \textbf{ mod } m = (b^{n/2} \textbf{ mod } m)^2 \textbf{ mod } m$$

quand n est pair et

$$b^n \textbf{ mod } m = \left((b^{\lfloor n/2 \rfloor} \textbf{ mod } m)^2 \textbf{ mod } m \cdot b \textbf{ mod } m \right) \textbf{ mod } m$$

lorsque n est impair, que nous décrivons dans le pseudocode comme l'algorithme 4.

Nous suivons l'exécution de l'algorithme 4 avec l'entrée $b = 2$, $n = 5$ et $m = 3$ pour illustrer comment Ça marche. Tout d'abord, parce que $n = 5$ est impair, nous utilisons la clause «else» pour voir que *mpower* (2, 5, 3) = (*mpower* (2, 2, 3)^2 **mod** 3 · 2 **mod** 3) **mod** 3. Nous utilisons ensuite la clause "else if" pour voir que *mpower* (2, 2, 3) = *mpower* (2, 1, 3)^2 **mod** 3. En utilisant à nouveau la clause «else», nous voyons que *mpower* (2, 1, 3) = (*mpower* (2, 0, 3)^2 **mod** 3 · 2 **mod** 3) **mod** 3. Enfin, en utilisant la clause "if", on voit que *mpower* (2, 0, 3) = 1. En reculant, il s'ensuit que *mpower* (2, 1, 3) = (1^2 **mod** 3 · 2 **mod** 3) **mod** 3 = 2, donc *mpower* (2, 2, 3) = 2^2 **mod** 3 = 1, et enfin *mpower* (2, 5, 3) = (1^2 **mod** 3 · 2 **mod** 3) **mod** 3 = 2. ▲

ALGORITHME 4 Exponentiation modulaire récursive.

procédure *mpower* (b , n , m : entiers avec b> 0 et $m \geq 2$, $n \geq 0$)
si $n = 0$ **alors**
  retour 1
sinon si n est encore **alors**
  retour *mpower (b, n / 2 , m)* ^{2} **mod** m
autre
  retour *(mpuissance (b,* $\lfloor n/2 \rfloor$ *, m)* ^{2} **mod** $m \cdot b$ **mod** *m)* **mod** m
{la sortie est b^n **mod** m }

Nous allons maintenant donner des versions récursives des algorithmes de recherche introduits dans la section 3.1.

EXEMPLE 5 Exprimer l'algorithme de recherche linéaire comme une procédure récursive.

Solution: Pour la *recherche* de la première occurrence de x dans la séquence d' un_1 , un_2 , ..., a_n , à la i ème étape de l'algorithme, x et a_i sont comparés. Si x est égal à a_i , l'algorithme renvoie i , l'emplacement de x dans la séquence. Sinon, la recherche de la première occurrence de x est réduite à une recherche dans une séquence avec un élément de moins, à savoir la séquence a_{i+1} , ..., a_n . L'algorithme retourne 0 lorsque x n'est jamais trouvé dans la séquence après examen de tous les termes. Nous pouvons maintenant donner une procédure récursive, qui est affichée comme pseudocode dans l'algorithme 5.

Soit *search (i, j, x)* la procédure qui recherche la première occurrence de x dans la séquence a_i , a_{i+1} , ..., a_j . L'entrée de la procédure se compose du triple *(1 , n, x)* . L'algorithme se termine à une étape si le premier terme de la séquence restante est x ou s'il n'y a qu'un seul terme de la séquence et ce n'est pas x . Si x n'est pas le premier terme et qu'il existe des termes supplémentaires, le même est effectuée mais avec une séquence de recherche d'un terme de moins, obtenue en supprimant le premier terme de la séquence de recherche. Si l'algorithme se termine sans que x ait été trouvé, le l'algorithme renvoie la valeur 0. ▲

ALGORITHME 5 Un algorithme de recherche linéaire récursif.

recherche de **procédure** *(i, j, x* : *i, j, x* entiers, $1 \leq i \leq j \leq n$)
si $a_i = x$ **alors**
  retour *je*
sinon si $i = j$ **alors**
  retour 0
autre
  retourner la *recherche (i* + 1 *, j, x)*
{sortie est l'emplacement de x dans un_1 , un_2 , ..., un_n s'il apparaît; sinon c'est 0}

EXEMPLE 6 Construisez une version récursive d'un algorithme de recherche binaire.

Solution: Supposons que nous voulons localiser x dans la séquence a_1 , a_2 , ..., a_n d'entiers en augmentant commande. Pour effectuer une recherche binaire, nous commençons par comparer x au terme moyen, $a_{\lfloor (n+1)/2 \rfloor}$. Notre algorithme se terminera si x est égal à ce terme et retournera l'emplacement de ce terme dans le séquence. Sinon, nous réduisons la recherche à une séquence de recherche plus petite, à savoir la première moitié de la séquence si x est plus petit que le terme moyen de la séquence d'origine, et la seconde la moitié sinon. Nous avons réduit la solution du problème de recherche à la solution du même

problème avec une séquence au moins deux fois plus longue. Si nous n'avons jamais rencontré le terme de recherche x , notre algorithme renvoie la valeur 0. Nous exprimons cette version récursive d'un algorithme de recherche binaire comme algorithme 6. ▲

ALGORITHME 6 Un algorithme de recherche binaire récursif.

procédure *recherche binaire (i, j, x* : *i, j, x* entiers, $1 \leq i \leq j \leq n$)
$m := \lfloor (i+j)/2 \rfloor$
si $x = a_m$ **alors**
  retour m
sinon si *(x <a* $_m$ et *i <m)* **alors**
  retourner *la recherche binaire (i, m* - 1 *, x)*
sinon si *(x> a* $_m$ et *j> m)* **alors**
  retourner *la recherche binaire (m* + 1 *, j, x)*
sinon retourne 0
{la sortie est l'emplacement de x dans un_1 , un_2 , ..., un_n s'il apparaît; sinon c'est 0}

Prouver les algorithmes récursifs corrects

L'induction mathématique, et sa variante forte induction, peuvent être utilisées pour prouver qu'un récursif l'algorithme est correct, c'est-à-dire qu'il produit la sortie souhaitée pour toutes les valeurs d'entrée possibles. Les exemples 7 et 8 illustrent comment l'induction mathématique ou l'induction forte peut être utilisée prouver que les algorithmes récursifs sont corrects. Tout d'abord, nous montrerons que l'algorithme 2 est correct.

EXEMPLE 7 Prouver que l'algorithme 2, qui calcule les puissances des nombres réels, est correct.

Solution: Nous utilisons l'induction mathématique sur l'exposant n .

ÉTAPE DE BASE: Si $n = 0$, la première étape de l'algorithme nous dit que la $puissance\ (a, 0) = 1$. C'est correct car $un_0 = 1$ pour chaque nombre réel non nul a . Ceci termine l'étape de base.

ÉTAPE INDUCTIVE: L'hypothèse inductive est la déclaration que la $puissance\ (a, k) = a^k$ pour tous $a = 0$ pour un entier non négatif arbitraire k . Autrement dit, l'hypothèse inductive est la déclaration que l'algorithme calcule correctement un^k . Pour terminer l'étape inductive, nous montrons que si le l'hypothèse inductive est vraie, alors l'algorithme calcule correctement un^{k+1} . Parce que $k + 1$ est un entier positif, lorsque l'algorithme calcule un^{k+1}, l'algorithme définit la $puissance\ (a, k + 1) = a \cdot puissance\ (a, k)$. Par l'hypothèse inductive, nous avons la $puissance\ (a, k) = a^k$, donc $puissance\ (a, k + 1) = a \cdot puissance\ (a, k) = a \cdot a^k = a^{k+1}$. Ceci termine l'étape inductive.

Nous avons terminé l'étape de base et l'étape inductive, nous pouvons donc conclure que l'algorithme 2 calcule toujours un^n correctement lorsque $a = 0$ et n est un entier non négatif. ▲

Généralement, nous devons utiliser une forte induction pour prouver que les algorithmes récursifs sont corrects, plutôt qu'une simple induction mathématique. L'exemple 8 illustre cela; il montre la forte induction peut être utilisé pour prouver que l'algorithme 4 est correct.

EXEMPLE 8 Prouver que l'algorithme 4, qui calcule les puissances modulaires, est correct.

Solution: Nous utilisons une forte induction sur l'exposant n .

ÉTAPE DE BASE: Soit b un entier et m un entier avec $m \geq 2$. Lorsque $n = 0$, l'algorithme définit $mpower\ (b, n, m)$ égal à 1. Ceci est correct car $b^0 \textbf{ mod } m = 1$. L'étape de base est terminée.

ÉTAPE INDUCTIVE: Pour l'hypothèse inductive, nous supposons que $mpower\ (b, j, m) = b^j \textbf{ mod } m$ pour tous les entiers $0 \leq j < k$ chaque fois que b est un entier positif et m est un entier avec $m \geq 2$. Pour terminer l'étape inductive, nous montrons que si l'hypothèse inductive est correcte, alors $mpuissance\ (b, k, m) = b^k \textbf{ mod } m$. Parce que l'algorithme récursif gère les valeurs paires et impaires de k différemment, nous divisons l'étape inductive en deux cas.

Lorsque k est pair, nous avons

$$mpower\ (b, k, m) = (mpower\ (b, k/2, m))^2 \textbf{ mod } m = (b^{k/2} \textbf{ mod } m)^2 \textbf{ mod } m = b^k \textbf{ mod } m,$$

où nous avons utilisé l'hypothèse inductive pour remplacer $mpower\ (b, k/2, m)$ par $b^{k/2} \textbf{ mod } m$.

Lorsque k est impair, nous avons

$$\begin{aligned} mpuissance\ (b, k, m) &= ((mpuissance\ (b, \lfloor k/2 \rfloor, m))^2 \textbf{ mod } m \cdot b \textbf{ mod } m) \textbf{ mod } m \\ &= ((b^{\lfloor k/2 \rfloor} \textbf{ mod } m)^2 \textbf{ mod } m \cdot b \textbf{ mod } m) \textbf{ mod } m \\ &= b^{2\lfloor k/2 \rfloor + 1} \textbf{ mod } m = b^k \textbf{ mod } m, \end{aligned}$$

en utilisant le corollaire 2 de la section 4.1, car $2\lfloor k/2 \rfloor + 1 = 2(k - 1)/2 + 1 = k$ lorsque k est impair. Ici, nous avons utilisé l'hypothèse inductive pour remplacer $mpower\ (b, \lfloor k/2 \rfloor, m)$ par $b^{\lfloor k/2 \rfloor} \textbf{ mod } m$. Ceci termine l'étape inductive.

Nous avons terminé l'étape de base et l'étape inductive, donc par forte induction, nous savons que l'algorithme 4 est correct. ▲

Récursivité et itération

Une définition récursive exprime la valeur d'une fonction à un entier positif en termes de valeurs de la fonction à des entiers plus petits. Cela signifie que nous pouvons concevoir un algorithme récursif pour évaluer une fonction définie récursivement à un entier positif. Au lieu de réduire successivement la calcul à l'évaluation de la fonction à des entiers plus petits, nous pouvons commencer par la valeur de la fonctionner à un ou plusieurs entiers, les cas de base, et appliquer successivement la définition récursive à

trouver les valeurs de la fonction à des entiers successifs plus grands. Une telle procédure est appelée **itérative** .
Souvent, une approche itérative pour l'évaluation d'une séquence définie récursivement nécessite beaucoup moins de calcul qu'une procédure utilisant la récursivité (à moins que les machines récursives à usage spécial sont utilisés). Ceci est illustré par les procédures itératives et récursives pour trouver le *n* ème Fibonacci nombre. La procédure récursive est donnée en premier.

ALGORITHME 7 Un algorithme récursif pour les nombres de Fibonacci.

procédure *Fibonacci* (*n* : entier positif)
si *n* = 0 **alors retourne** 0
sinon si *n* = 1 **alors retourne** 1
sinon retourner *fibonacci (n* - 1 *)* + *fibonacci (n* - 2 *)*
{la sortie est *fibonacci (n)* }

Lorsque nous utilisons une procédure récursive pour trouver f_n , nous exprimons d'abord f_n comme $f_{n-1} + f_{n-2}$. Ensuite nous remplacer ces deux numéros de Fibonacci par la somme de deux numéros de Fibonacci précédents, et bientôt. Lorsque f_1 ou f_0 apparaît, il est remplacé par sa valeur.

Notez qu'à chaque étape de la récursivité, jusqu'à ce que f_1 ou f_0 soit obtenu, le nombre de Fibonacci le nombre à évaluer a doublé. Par exemple, lorsque nous trouvons f_4 en utilisant cette algo récursive rithme, nous devons effectuer tous les calculs illustrés dans l'arborescence de la figure 1. Cette

f_4

f_3 f_2

f_2 f_1 f_1 f_0

f_1 f_0

FIGURE 1 **Évaluation de f_4 récursivement.**

l'arbre se compose d'une racine étiquetée avec f_4 et de branches de la racine aux sommets étiquetés avec le deux nombres de Fibonacci f_3 et f_2 qui interviennent dans la réduction du calcul de f_4 . Chaque la réduction subséquente produit deux branches dans l'arbre. Cette ramification se termine lorsque f_0 et f_1 sont atteints. Le lecteur peut vérifier que cet algorithme nécessite f_{n+1} - 1 ajouts pour trouver f_n .

Considérons maintenant la quantité de calcul nécessaire pour trouver f_n en utilisant l'approche itérative dans l'algorithme 8.

ALGORITHME 8 Un algorithme itératif pour calculer les nombres de Fibonacci.

procédure *fibonacci itérative* (*n* : entier non négatif)
si *n* = 0 **alors retourne** 0
autre
  x : = 0
  y : = 1
  pour *i* : = 1 à *n* - 1
    z : = *x* + *y*
    x : = *y*
    y : = *z*
  retourner *y*
{la sortie est le *n* ème numéro de Fibonacci}

Cette procédure initialise *x* comme $f_0 = 0$ et *y* comme $f_1 = 1$. Lorsque la boucle est parcourue, la somme de *x* et *y* est affecté à la variable auxiliaire *z* . Ensuite, *x* reçoit la valeur de *y* et *y* est attribué la valeur de la variable auxiliaire *z* . Par conséquent, après avoir parcouru la boucle la première fois, il il s'ensuit que *x* est égal à f_1 et *y* est égal à $f_0 + f_1 = f_2$. De plus, après avoir parcouru la boucle *n* - 1 fois, *x* est égal à f_{n-1} et *y* est égal à f_n (le lecteur doit vérifier cette déclaration). Seulement *n* - 1 des additions ont été utilisées pour trouver f_n avec cette approche itérative lorsque n> 1. Par conséquent, cette L'algorithme nécessite beaucoup moins de calculs que l'algorithme récursif.

Nous avons montré qu'un algorithme récursif peut nécessiter beaucoup plus de calculs qu'un itératif une lorsqu'une fonction définie de manière récursive est évaluée. Il est parfois préférable d'utiliser un récursif même si elle est moins efficace que la procédure itérative. En particulier, cela est vrai lorsque l'approche récursive est facilement mise en œuvre et l'approche itérative ne l'est pas. (Aussi, les machines conçu pour gérer la récursivité peut être disponible pour éliminer l'avantage de l'itération.)

8 2 4 6 9 7 10 1 5 3

8 2 4 6 9 7 10 1 5 3

8 2 4 6 9 7 10 1 5 3

8 2 4 6 9 7 10 1 5 3

8 2 sept dix

8 2 sept dix

2 8 4 6 9 7 10 1 5 3

2 4 8 6 9 1 7 10 3 5

2 4 6 8 9 1 3 5 7 10

1 2 3 4 5 6 7 8 9 10

FIGURE 2 Le tri par fusion de 8, 2, 4, 6, 9, 7, 10, 1, 5, 3.

Le tri par fusion

Nous décrivons maintenant un algorithme de tri récursif appelé algorithme de tri par **fusion** . Nous allons démontrer expliquez comment l'algorithme de tri par fusion fonctionne avec un exemple avant de le décrire en général.

EXEMPLE 9 Utilisez le tri par fusion pour mettre les termes de la liste 8, 2, 4, 6, 9, 7, 10, 1, 5, 3 dans l'ordre croissant.

Solution: un tri par fusion commence par fractionner la liste en éléments individuels en successivement diviser les listes en deux. La progression des sous-listes pour cet exemple est représentée par l'équilibre arbre binaire de hauteur 4 montré dans la moitié supérieure de la figure 2.

Le tri se fait en fusionnant successivement des paires de listes. Au premier stade, des paires de les éléments sont fusionnés dans des listes de longueur deux dans l'ordre croissant. Puis des fusions successives de des paires de listes sont effectuées jusqu'à ce que la liste entière soit mise en ordre croissant. La succession de les listes fusionnées dans l'ordre croissant sont représentées par l'arbre binaire équilibré de hauteur 4 montré dans la moitié inférieure de la figure 2 (notez que cet arbre est affiché «à l'envers»). ▲

En général, un tri par fusion procède par division itérative des listes en deux sous-listes d'égales longueur (ou lorsqu'une sous-liste a un élément de plus que l'autre) jusqu'à ce que chaque sous-liste en contienne un élément. Cette succession de sous-listes peut être représentée par un arbre binaire équilibré. La procédure continue en fusionnant successivement des paires de listes, où les deux listes sont en ordre croissant, en un liste plus grande avec les éléments dans l'ordre croissant, jusqu'à ce que la liste d'origine soit mise dans l'ordre croissant. La succession de listes fusionnées peut être représentée par un arbre binaire équilibré.

Nous pouvons également décrire le tri par fusion de manière récursive. Pour effectuer un tri par fusion, nous avons divisé une liste en deux sous-listes de taille égale ou approximativement égale, triant chaque sous-liste à l'aide du tri par fusion algorithme, puis fusionner les deux listes. La version récursive du tri par fusion est donnée dans Algorithme 9. Cet algorithme utilise la *fusion de* sous-programmes , qui est décrite dans l'algorithme 10.

ALGORITHME 9 Un tri récursif par fusion.

mergesort de **procédure** *(L* = $a_1, \ldots, a_n$*)*
si $n > 1$ **alors**
  $m := \lfloor n/2 \rfloor$
  $L_1 := a_1, a_2, \ldots, a_m$
  $L_2 := a_{m+1}, a_{m+2}, \ldots, a_n$
  L := *fusion (mergesort* (L_1)*, mergesort* (L_2)*)*
{ L est maintenant trié en éléments dans un ordre non décroissant}

Un algorithme efficace pour fusionner deux listes ordonnées en une liste ordonnée plus grande est nécessaire pour implémenter le tri par fusion. Nous allons maintenant décrire une telle procédure.

EXEMPLE 10 Fusionnez les deux listes 2, 3, 5, 6 et 1, 4.

Solution: le tableau 1 illustre les étapes que nous utilisons. Tout d'abord, comparez les plus petits éléments des deux listes, 2 et 1, respectivement. Parce que 1 est le plus petit, mettez-le au début de la liste fusionnée et supprimez-le de la deuxième liste. À ce stade, la première liste est 2, 3, 5, 6, la seconde est 4 et la liste combinée est 1.

Ensuite, comparez 2 et 4, les plus petits éléments des deux listes. Parce que 2 est le plus petit, ajoutez à la liste combinée et supprimez-le de la première liste. A ce stade, la première liste est 3, 5, 6, le le second est 4, et la liste combinée est 1, 2.

Continuez en comparant 3 et 4, les plus petits éléments de leurs listes respectives. Parce que 3 est le plus petit de ces deux éléments, ajoutez-le à la liste combinée et supprimez-le de la première liste. À ce stade, la première liste est 5, 6 et la seconde est 4. La liste combinée est 1, 2, 3.

Comparez ensuite 5 et 4, les plus petits éléments des deux listes. Parce que 4 est le plus petit de ces deux éléments, ajoutez-le à la liste combinée et supprimez-le de la deuxième liste. À ce stade la première liste est 5, 6, la deuxième liste est vide et la liste combinée est 1, 2, 3, 4.

Enfin, comme la deuxième liste est vide, tous les éléments de la première liste peuvent être ajoutés à la fin de la liste combinée dans l'ordre dans lequel ils apparaissent dans la première liste. Cela produit l'ordre liste 1, 2, 3, 4, 5, 6. ▲

Nous allons maintenant considérer le problème général de la fusion de deux listes ordonnées L_1 et L_2 en une liste ordonnée L . Nous décrirons un algorithme pour résoudre ce problème. Commencez avec un vide liste L . Comparez les plus petits éléments des deux listes. Mettez le plus petit de ces deux éléments à l'extrémité droite de L , et supprimez-la de la liste dans laquelle elle se trouvait. Ensuite, si l'un des L_1 et L_2 est vide, ajoutez l'autre liste (non vide) à L , ce qui termine la fusion. Si ni L_1 ni L_2 n'est vide, répétez ce processus. L'algorithme 10 donne une description de pseudocode de cette procédure.

TABLEAU 1 **Fusion des deux listes triées 2, 3, 5, 6 et 1, 4.**

Première liste	*Deuxième liste*	*Liste fusionnée*	*Comparaison*
2356	14		1 < 2
2356	4	1	2 < 4
356	4	12	3 < 4
56	4	123	4 < 5
56		1234	
		123456	

Nous aurons besoin d'estimations du nombre de comparaisons utilisées pour fusionner deux listes ordonnées analyse du tri par fusion. Nous pouvons facilement obtenir une telle estimation pour l'algorithme 10. À chaque fois une comparaison d'un élément de L_1 et d'un élément de L_2 est effectuée, un élément supplémentaire est ajouté à la liste fusionnée L. Cependant, lorsque L_1 ou L_2 est vide, plus de comparaisons sont nécessaires. Par conséquent, l'algorithme 10 est le moins efficace lorsque $m + n - 2$ comparaisons sont effectuées, où m et n sont le nombre d'éléments dans L_1 et L_2, respectivement, laissant un élément dans chacun de L_1 et L_2. La prochaine comparaison sera la dernière nécessaire, car elle en fera une de ces listes vides. Par conséquent, l'algorithme 10 n'utilise pas plus de $m + n - 1$ comparaisons. Lemme 1 résume cette estimation.

ALGORITHME 10 Fusion de deux listes.

fusion de **procédure** *(L_1, L_2* : listes triées *)*
L : = liste vide

tandis que L_1 et L_2 sont tous deux non vides
  retirer le plus petit des premiers éléments de L_1 et L_2 de sa liste; le mettre à l'extrémité droite de L
  si ce retrait fait une liste vide **puis** supprimer tous les éléments de l'autre liste et
    les ajouter à L
return L { L est la liste fusionnée avec les éléments dans l'ordre croissant}

LEMMA 1 Deux listes triées avec m éléments et n éléments peuvent être fusionnées en une liste triée en utilisant no plus de $m + n - 1$ comparaisons.

Parfois, deux listes triées de longueur m et n peuvent être fusionnées en utilisant bien moins que $m + n - 1$ comparaisons. Par exemple, lorsque $m = 1$, une procédure de recherche binaire peut être appliquée pour mettre un élément de la première liste dans la deuxième liste. Cela ne nécessite que des comparaisons $\lceil \log n \rceil$, qui est beaucoup plus petit que $m + n - 1 = n$, pour $m = 1$. Par contre, pour certaines valeurs de m et n, le lemme 1 donne la meilleure borne possible. Autrement dit, il existe des listes avec m et n éléments qui ne peuvent pas être fusionnés en utilisant moins de $m + n - 1$ comparaisons. (Voir l'exercice 47.)

Nous pouvons maintenant analyser la complexité du tri par fusion. Au lieu d'étudier le général problème, nous supposerons que n, le nombre d'éléments dans la liste, est une puissance de 2, disons 2^m. Cette rendra l'analyse moins compliquée, mais lorsque ce n'est pas le cas, diverses modifications peuvent être appliqué qui donnera la même estimation.

Au premier stade de la procédure de fractionnement, la liste est divisée en deux sous-listes, de 2^{m-1} éléments chacun, au niveau 1 de l'arbre généré par le fractionnement. Ce processus se poursuit, divisant les deux sous-listes avec 2^{m-1} éléments en quatre sous-listes de 2^{m-2} éléments au niveau 2, etc. Dans général, il y a 2^{k-1} listes au niveau $k - 1$, chacune avec 2^{m-k+1} éléments. Ces listes au niveau $k - 1$ sont divisés en 2^k listes au niveau k, chacune avec 2^{m-k} éléments. À la fin de ce processus, nous avons 2^m répertorie chacun avec un élément au niveau m.

Nous commençons à fusionner en combinant des paires des 2^m listes d'un élément en 2^{m-1} listes, au niveau $m - 1$, chacun avec deux éléments. Pour ce faire, 2^{m-1} des paires de listes avec un élément chacune sont fusionnées. La fusion de chaque paire nécessite exactement une comparaison.

La procédure se poursuit, de sorte qu'au niveau k $(k = m, m - 1, m - 2, \ldots, 3, 2, 1)$, 2^k listes chacun avec 2^{m-k} les éléments sont fusionnés en 2^{k-1} listes, chacune avec 2^{m-k+1} éléments, au niveau $k - 1$. Pour ce faire, un total de 2^{k-1} fusion de deux listes, chacune avec 2^{m-k} éléments, sont nécessaires. Mais, par le lemme 1, chacune de ces fusions peut être réalisée en utilisant au plus $2^{m-k} + 2^{m-k} - 1 = 2^{m-k+1} - 1$ comparaisons. Par conséquent, passer du niveau k à $k - 1$ peut être accompli en utilisant au plus $2^{k-1}(2^{m-k+1} - 1)$ comparaisons.

La somme de toutes ces estimations montre que le nombre de comparaisons requises pour la fusion le tri est tout au plus

$$\sum_{k=1}^{m} 2^{k-1}(2^{m-k+1} - 1) = \sum_{k=1}^{m} 2^{m} - \sum_{k=1}^{m} 2^{k-1} = m2^{m} - (2^{m} - 1) = n \log n - n + 1,$$

car $m = \log n$ et $n = 2^{m}$. (Nous avons évalué $\sum_{k=1}^{m} 2^{m}$ en notant que c'est la somme de m termes identiques, chacun égal à 2^{m}. Nous avons évalué $\sum_{k=1}^{m} 2^{k-1}$ en utilisant la formule pour la somme de les termes d'une progression géométrique du théorème 1 de la section 2.4.)

Le théorème 1 résume ce que nous avons découvert au sujet de la complexité la plus défavorable du fusionner l'algorithme de tri.

THÉORÈME 1 Le nombre de comparaisons nécessaires pour fusionner trier une liste avec n éléments est $O(n \log n)$.

Au chapitre 11, nous montrerons que l'algorithme de tri basé sur la comparaison le plus rapide $O(n \log n)$ complexité temporelle. (Un algorithme de tri basé sur la comparaison a la comparaison de deux éléments comme son fonctionnement de base.) Le théorème 1 nous dit que le tri par fusion atteint ce meilleur estimation big- O possible de la complexité d'un algorithme de tri. Nous décrivons un autre efficace algorithme, le tri rapide, dans le préambule de l'exercice 50.

Des exercices

1. Tracez l'algorithme 1 lorsqu'il reçoit $n = 5$ en entrée. Cette est, afficher toutes les étapes utilisées par l'algorithme 1 pour trouver 5 !, comme c'est fait dans l'exemple 1 pour en trouver 4 !.

2. Tracez l'algorithme 1 lorsqu'il reçoit $n = 6$ en entrée. Cette est, afficher toutes les étapes utilisées par l'algorithme 1 pour trouver 6 !, comme c'est fait dans l'exemple 1 pour en trouver 4 !.

3. Tracez l'algorithme 3 lorsqu'il trouve gcd $(8, 13)$. Autrement dit, montrer toutes les étapes utilisées par l'algorithme 3 pour trouver gcd $(8, 13)$.

4. Tracez l'algorithme 3 lorsqu'il trouve gcd $(12, 17)$. C'est, montrer toutes les étapes utilisées par l'algorithme 3 pour trouver gcd $(12, 17)$.

5. Trace l'algorithme 4 quand on lui donne $m = 5$, $n = 11$, et $b = 3$ en entrée. Autrement dit, affichez toutes les étapes Algorithme 4 utilise pour trouver 3^{11} **mod** 5.

6. Trace l'algorithme 4 quand on lui donne $m = 7$, $n = 10$, et $b = 2$ en entrée. Autrement dit, affichez toutes les étapes Algorithme 4 utilise pour trouver 2^{10} **mod** 7.

7. Donner un algorithme récursif pour calculer nx chaque fois que n est un entier positif et x est un entier, en utilisant simplement l'addition.

8. Donnez un algorithme récursif pour trouver la somme des n premiers entiers positifs.

9. Donnez un algorithme récursif pour trouver la somme des premiers n entiers positifs impairs.

10. Donnez un algorithme récursif pour trouver le maximum de un ensemble fini d'entiers, en utilisant le fait que le maximum de n entiers est le plus grand du dernier entier la liste et le maximum des $n - 1$ premiers nombres entiers dans le liste.

11. Donnez un algorithme récursif pour trouver le minimum d'un ensemble fini d'entiers, en utilisant le fait que le nombre imum de n entiers est le plus petit du dernier entier de la liste et le minimum des $n - 1$ premiers entiers de la liste.

12. Concevoir un algorithme récursif pour trouver x^{n} **mod** m quand-jamais n, x et m sont des entiers positifs basés sur le fait que x^{n} **mod** $m = (x^{n-1}$ **mod** $m \cdot x$ **mod** $m)$ **mod** m.

13. Donnez un algorithme récursif pour trouver n ! **mod** m quand-toujours n et m sont des entiers positifs.

14. Donnez un algorithme récursif pour trouver un **mode** d'une liste de entiers. (Un **mode** est un élément de la liste qui se produit à moins souvent que tous les autres éléments.)

15. Concevoir un algorithme récursif pour calculer le plus grand diviseur commun de deux entiers non négatifs a et b avec $a < b$ en utilisant le fait que gcd $(a, b) =$ gcd $(a, b - a)$.

16. Démontrer que l'algorithme récursif pour trouver la somme de les n premiers entiers positifs que vous avez trouvés dans l'exercice 8 sont correct.

17. Décrire un algorithme récursif pour multiplier deux non entiers négatifs x et y basés sur le fait que $xy =$

38. Donner un algorithme récursif pour trouver la chaîne w^{je}, les concaténation de i copies de w, lorsque w est une chaîne de bits.

$2(x \cdot (y/2))$ lorsque y est pair et $xy = 2(x \cdot \lfloor y/2 \rfloor) + x$ lorsque y est impair, avec la condition initiale $xy = 0$ lorsque $y = 0$.

18. Prouvez que l'algorithme 1 pour calculer $n\,!$ quand n est un non un entier négatif est correct.

19. Démontrer que l'algorithme 3 pour calculer le pgcd (a, b) quand a et b sont des entiers positifs avec $a < b$ est correct.

20. Prouvez que l'algorithme que vous avez conçu dans l'exercice 17 est correct.

21. Prouvez que l'algorithme récursif que vous avez trouvé dans Ex- l'exercice 7 est correct.

22. Prouvez que l'algorithme récursif que vous avez trouvé dans Ex- l'exercice 10 est correct.

23. Concevoir un algorithme récursif pour calculer n^2 où n est un entier non négatif, en utilisant le fait que $(n+1)^2 = n^2 + 2n + 1$. Démontrez ensuite que cet algorithme est correct.

24. Concevoir un algorithme récursif pour trouver un^{2^n}, où a est un nombre réel et n est un entier positif. [*Astuce:* utilisez le égalité $a^{2^{n+1}} = (a^{2^n})^2$.]

25. Comment le nombre de multiplications utilisé par l'al- gorithme de l'exercice 24 par rapport au nombre de plications utilisées par l'algorithme 2 pour évaluer un^{2^n}?

* **26.** Utilisez l'algorithme de l'exercice 24 pour concevoir un algo- rithme pour évaluer un^n lorsque n est un entier non négatif. [*Astuce:* utilisez l'expansion binaire de n .]

* **27.** Comment le nombre de multiplications utilisé par l'al- gorithme de l'exercice 26 par rapport au nombre de plications utilisées par l'algorithme 2 pour évaluer un^n?

28. Combien d'additions sont utilisées par la récursive et l'itération algorithmes efficaces donnés dans les algorithmes 7 et 8, respectivement, trouver le nombre de Fibonacci f_7 ?

29. Concevoir un algorithme récursif pour trouver le n ème terme de la séquence définie par $a_0 = 1$, $a_1 = 2$, et $a_n = a_{n-1} \cdot a_{n-2}$, pour $n = 2, 3, 4, \ldots$.

30. Concevoir un algorithme itératif pour trouver le n ème terme du séquence définie dans l'exercice 29.

31. L'algorithme récursif ou itératif pour trouver le séquence de l'exercice 29 plus efficace?

32. Concevoir un algorithme récursif pour trouver le n ème terme de la séquence définie par $un_0 = 1$, $un_1 = 2$, $un_2 = 3$, et $a_n = a_{n-1} + a_{n-2} + a_{n-3}$, pour $n = 3, 4, 5, \ldots$.

33. Concevoir un algorithme itératif pour trouver le n ème terme du séquence définie dans l'exercice 32.

34. Est-ce l'algorithme récursif ou itératif pour trouver le séquence de l'exercice 32 plus efficace?

35. Donner des algorithmes itératifs et récursifs pour trouver le n ème terme de la séquence définie par $a_0 = 1$, $a_1 = 3$, $a_2 = 5$, et $a_n = a_{n-1} \cdot a_{n-2}^2 \cdot a_{n-3}^3$. Quel est le plus efficace?

36. Donnez un algorithme récursif pour trouver le nombre de tions d'un entier positif basé sur la définition récursive donnée dans l'exercice 47 de la section 5.3.

37. Donner un algorithme récursif pour trouver l'inversion d'un bit chaîne. (Voir la définition de l'inversion d'une chaîne de bits dans le préambule de l'exercice 34 de la section 5.3.)

39. Prouver que l'algorithme récursif pour trouver l'inversion d'une chaîne de bits que vous avez donnée dans l'exercice 37 est correcte.

40. Montrer que l'algorithme récursif pour trouver la concaténation nation de i copies d'une chaîne de bits que vous avez donnée dans l'exercice 38 est correct.

* **41.** Donner un algorithme récursif pour paver un $2^n \times 2^n$ vérificateur- planche avec un carré manquant en utilisant des triominos droits.

42. Donner un algorithme récursif pour trianguler un poly- gon avec n côtés, en utilisant le lemme 1 dans la section 5.2.

43. Donner un algorithme récursif pour calculer les valeurs de la Fonction Ackermann. [*Astuce:* Voir le préambule de Exer- cise 48 dans la section 5.3.]

44. Utilisez un tri par fusion pour trier 4, 3, 2, 5, 1, 8, 7, 6 en commande. Affiche toutes les étapes utilisées par l'algorithme.

45. Utilisez un tri par fusion pour trier *b, d, a, f, g, h, z, p, o, k* en al- ordre phabétique. Affiche toutes les étapes utilisées par l'algorithme.

46. Combien de comparaisons sont nécessaires pour fusionner ces paires de listes utilisant l'algorithme 10?

a) 1, 3, 5, 7, 9; 2, 4, 6, 8, 10

b) 1, 2, 3, 4, 5; 6, 7, 8, 9, 10

c) 1, 5, 6, 7, 8; 2, 3, 4, 9, 10

47. Montrer que pour tous les entiers positifs m et n il y a tri listes avec m éléments et n éléments, respectivement, telles que l'algorithme 10 utilise $m + n - 1$ comparaisons pour fusionner les en une seule liste triée.

* **48.** Quel est le moins de comparaisons nécessaires pour fusionner deux listes dans l'ordre croissant en une seule liste en augmentant l'ordre lorsque le nombre d'éléments dans les deux listes est

a) 1, 4? **b)** 2, 4? **c)** 3, 4? **d)** 4, 4?

* **49.** Prouvez que l'algorithme de tri par fusion est correct.

Le **tri rapide** est un algorithme efficace. Trier $a_1, a_2, \ldots, a_n$, cet algorithme commence par prendre la première élément a_1 et formant deux sous-listes, le premier contenant ing ces éléments qui sont inférieurs à un_1, dans l'ordre surgir, et le second contenant ces éléments plus que d' un_1, dans l'ordre où ils se présentent. Ensuite, un_1 est mis à la fin de la première sous-liste. Cette procédure est répétée récursivement pour chaque sous-liste, jusqu'à ce que toutes les sous-listes contiennent un élément. L'or- La liste dérivée de n éléments est obtenue en combinant les sous-listes d'un élément dans l'ordre où ils se produisent.

50. Triez 3, 5, 7, 8, 1, 9, 2, 4, 6 en utilisant le tri rapide.

51. Soit $a_1, a_2, \ldots, a_n$ une liste de n nombres réels distincts. Combien de comparaisons sont nécessaires pour former deux sous-listes de cette liste, les premiers éléments contenant moins d' un_1 et le second contenant des éléments supérieurs à un_1 ?

52. Décrire l'algorithme de tri rapide en utilisant le pseudocode.

53. Quel est le plus grand nombre de comparaisons nécessaires pour der une liste de quatre éléments en utilisant l'algorithme de tri rapide?

54. Quel est le moins de comparaisons nécessaires pour commander une liste de quatre éléments utilisant l'algorithme de tri rapide?

55. Déterminer la complexité la plus défavorable du tri rapide algorithme en termes de nombre de comparaisons utilisées.

Exactitude du programme

introduction

Supposons que nous avons conçu un algorithme pour résoudre un problème et écrit un programme pour le mettre en œuvre. Comment être sûr que le programme produit toujours la bonne réponse? Une fois tous les bogues supprimés pour que la syntaxe soit correcte, nous pouvons tester le programme avec échantillon d'entrée. Il n'est pas correct si un résultat incorrect est produit pour une entrée d'échantillon. Mais même si le programme donne la bonne réponse pour toutes les entrées d'échantillon, il peut ne pas toujours produire la bonne réponse (sauf si toutes les entrées possibles ont été testées). Nous avons besoin d'une preuve pour montrer que le programme donne *toujours* la sortie correcte.

La vérification des programmes, la preuve de l'exactitude des programmes, utilise les règles d'inférence et les techniques de preuve décrites dans ce chapitre, y compris l'induction mathématique. Parce qu'une programme peut conduire à des résultats désastreux, une grande quantité de méthodologie a été construite

pour vérifier les programmes. Des efforts ont été consacrés à l'automatisation de la vérification des programmes afin
peut être effectuée à l'aide d'un ordinateur. Cependant, seuls des progrès limités ont été
objectif. En effet, certains mathématiciens et informaticiens théoriciens affirment qu'il ne sera jamais
être réaliste pour mécaniser la preuve d'exactitude de programmes complexes.

Certains concepts et méthodes utilisés pour prouver que les programmes sont corrects seront introduits dans cette section. De nombreuses méthodes différentes ont été conçues pour prouver que les programmes sont corrects. Nous discuterons d'une méthode largement utilisée pour la vérification de programme introduite par Tony Hoare dans cette section; plusieurs autres méthodes sont également couramment utilisées. De plus, nous ne développerons pas de méthodologie complète pour la vérification du programme dans ce livre. Cette section se veut un bref introduction au domaine de la vérification des programmes, qui relie les règles de logique, de preuve techniques et le concept d'un algorithme.

Vérification du programme

Un programme est considéré comme **correct** s'il produit la sortie correcte pour chaque entrée possible. Une preuve qu'un programme est correct se compose de deux parties. La première partie montre que la bonne réponse est obtenu si le programme se termine. Cette partie de la preuve établit l'**exactitude partielle** du programme. La deuxième partie de la preuve montre que le programme se termine toujours.

Pour spécifier ce que signifie pour un programme de produire la sortie correcte, deux propositions sont utilisés. La première est l' **assertion initiale** , qui donne les propriétés que les valeurs d'entrée doivent avoir. La seconde est l' **assertion finale** , qui donne les propriétés que la sortie du programme devrait avoir, si le programme a fait ce qui était prévu. Les assertions initiales et finales appropriées doit être fourni lors de la vérification d'un programme.

DÉFINITION 1 Un programme ou un segment de programme, S est dit être *partiellement correcte par rapport à* la assertion initiale p et assertion finale q si chaque fois que p est vrai pour les valeurs d'entrée de S et S se termine, alors q est vrai pour les valeurs de sortie de S . La notation $p\ \{S\}\ q$ in- indique que le programme ou le segment de programme S est partiellement correct par rapport au assertion p et assertion finale q .

Remarque: La notation $p\ \{S\}\ q$ est connue sous le nom de *triple de Hoare* . Tony Hoare a présenté le concept de exactitude partielle.

Notez que la notion de correction partielle n'a rien à voir avec le fait qu'un programme nates; il se concentre uniquement sur si le programme fait ce qu'il est censé faire s'il se termine.

Un exemple simple illustre les concepts des affirmations initiales et finales.

EXEMPLE 1 Montrer que le segment de programme

$y := 2$
$z := x + y$

est correcte par rapport à l'assertion initiale $p : x = 1$ et l'assertion finale $q : z = 3$.

Solution: Supposons que p soit vrai, de sorte que $x = 1$ au début du programme. Ensuite, y est affecté valeur 2, et z est affectée à la somme des valeurs de x et y , qui est 3. Par conséquent, S est correct avec par rapport à l'assertion initiale p et à l'assertion finale q . Ainsi, $p\ \{S\}\ q$ est vrai. ▲

Règles d'inférence

Une règle d'inférence utile prouve qu'un programme est correct en le divisant en un séquence de sous-programmes et montrant ensuite que chaque sous-programme est correct.

Supposons que le programme S soit divisé en sous-programmes S_1 et S_2 . Écrivez $S = S_1 ; S_2$ pour indiquer que S est composé de S_1 suivi de S_2 . Supposons que l'exactitude de S_1 par rapport à la assertion initiale p et assertion finale q , et l'exactitude de S_2 par rapport à l'initiale l'assertion q et l'assertion finale r ont été établies. Il s'ensuit que si p est vrai et S_1 est exécuté et se termine, alors q est vrai; et si q est vrai, et S_2 s'exécute et se termine, alors r est vrai. Ainsi, si p est vrai et $S = S_1 ; S_2$ est exécuté et se termine, alors r est vrai. Cette règle de L'inférence, appelée **règle de composition** , peut être formulée comme suit:

$$\begin{array}{l} p\ \{S_1\}\ q \\ q\ \{S_2\}\ r \\ \hline \therefore p\ \{S_1; S_2\}\ r. \end{array}$$

Cette règle d'inférence sera utilisée plus loin dans cette section.

Ensuite, quelques règles d'inférence pour les segments de programme impliquant des instructions conditionnelles et des boucles seront données. Étant donné que les programmes peuvent être divisés en segments pour des preuves d'exactitude, cela nous permettra de vérifier de nombreux programmes différents.

Expressions conditionnelles

Premièrement, des règles d'inférence pour les instructions conditionnelles seront données. Supposons qu'un programme segment a la forme

si *condition* **alors**
    S

où S est un bloc d'instructions. Alors S est exécuté si la *condition* est vraie, et il n'est pas exécuté lorsque la *condition* est fausse. Pour vérifier que ce segment est correct par rapport à l'assertion initiale p et affirmation finale q , deux choses doivent être faites. Tout d'abord, il faut montrer que lorsque p est vrai et *état* est également vrai, alors q est vrai après S se termine. Deuxièmement, il faut montrer que lorsque p est vrai et la *condition* est fausse, alors q est vrai (car dans ce cas S ne s'exécute pas).

Cela conduit à la règle d'inférence suivante:

$(condition\ p \wedge)\ \{S\}\ q$
$(condition\ p \wedge \neg) \rightarrow q$

$\therefore p\ \{$**si** *condition* **alors** $S\}\ q$.

L'exemple 2 illustre comment cette règle d'inférence est utilisée.

EXEMPLE 2 Vérifiez que le segment de programme

si $x > y$ **alors**
    $y := x$

est correcte par rapport à l'assertion initiale **T** et à l'assertion finale $y \geq x$.

Solution: Lorsque l'assertion initiale est vraie et $x > y$, l'affectation $y := x$ est effectuée. Par conséquent, l'assertion finale, qui affirme que $y \geq x$, est vraie dans ce cas. De plus, lorsque le l'assertion initiale est vraie et $x > y$ est fausse, de sorte que $x \leq y$, l'assertion finale est à nouveau vraie. Par conséquent, en utilisant la règle d'inférence pour les segments de programme de ce type, ce programme est correct en ce qui concerne aux affirmations initiales et finales données. ▲

De même, supposons qu'un programme ait une déclaration de la forme

si *condition* **alors**
    S_1
autre
    S_2

Si la *condition* est vraie, alors S_1 s'exécute; si la *condition* est fausse, alors S_2 s'exécute. Pour vérifier que cela le segment de programme est correct par rapport à l'assertion initiale p et à l'assertion finale q , deux il faut faire les choses. Tout d'abord, il faut montrer que lorsque p est vrai et que la *condition* est vraie, alors q est vrai après la fin de S_1 . Deuxièmement, il faut montrer que lorsque p est vrai et que la *condition* est fausse, alors q est vrai après la fin de S_2 . Cela conduit à la règle d'inférence suivante:

$(condition\ p \wedge)\ \{S_1\}\ q$
$(condition\ p \wedge \neg)\ \{S_2\}\ q$

$\therefore p\ \{$**si** *condition* **alors** S_1 **sinon** $S_2\}\ q$.

C. ANTHONY R. HOARE (NÉ EN 1934) Tony Hoare est né à Colombo, Ceylan (maintenant connu sous le nom de Sri Lanka), où son père était fonctionnaire de l'Empire britannique et le père de sa mère possédait une plantation. Il a passé sa petite enfance à Ceylan, s'installe en Angleterre en 1945. Hoare a étudié la philosophie, avec les classiques, à l'Université d'Oxford, où il s'est intéressé à l'informatique en raison de sa fascination avec la puissance de la logique mathématique et la certitude de la vérité mathématique. Il a obtenu son baccalauréat d'Oxford en 1956.

Hoare a appris le russe pendant son service dans la Royal Navy, et ce dernier a étudié la traduction informatique de langues naturelles à l'Université d'État de Moscou. Il est retourné en Angleterre en 1960, prenant un emploi dans un petit fabricant d'ordinateurs, où il a écrit un compilateur pour le langage de programmation Algol. En 1968, il est devenu professeur d'informatique au Queen's Université, Belfast; en 1977, il a rejoint l'Université d'Oxford en tant que professeur d'informatique; il est maintenant professeur émérite. Il est un Membre de la Royal Society et occupe également un poste chez Microsoft Research à Cambridge.

Hoare a apporté de nombreuses contributions à la théorie des langages de programmation et à la méthodologie de programmation. Il était le premier définir un langage de programmation basé sur la façon dont les programmes pourraient être prouvés par rapport à leurs spécifications. Hoare aussi a inventé le tri rapide, l'un des algorithmes de tri les plus couramment utilisés (voir le préambule de l'exercice 50 à la section 5.4). Il a reçu le prix ACM Turing en 1980 et en 2000, il a été fait chevalier pour ses services en éducation et en informatique. Hoare est un écrivain réputé dans les aspects techniques et sociaux de l'informatique.

L'exemple 3 illustre comment cette règle d'inférence est utilisée.

EXEMPLE 3 Vérifiez que le segment de programme

si $x < 0$ **alors**
    $abs := -x$
autre
    $abs := x$

est correcte par rapport à l'assertion initiale **T** et à l'assertion finale $abs = |x|$.

Solution: Deux choses doivent être démontrées. Tout d'abord, il faut montrer que si l'affirmation initiale est vrai et $x < 0$, puis $abs = |x|$. C'est correct, car lorsque $x < 0$ l'instruction d'affectation $abs := -x$ définit $abs = -x$, qui est $|x|$ par définition lorsque $x < 0$. Deuxièmement, il doit être affiché que si l'assertion initiale est vraie et $x < 0$ est fausse, de sorte que $x \geq 0$, alors $abs = |x|$. C'est aussi correct, car dans ce cas, le programme utilise l'instruction d'affectation $abs := x$, et x est $|x|$ par définition lorsque $x \geq 0$, donc $abs := x$. Par conséquent, en utilisant la règle d'inférence pour les segments de programme de ce type, ce segment est correct par rapport aux assertions initiales et finales données. ▲

Invariants de boucle

Ensuite, des preuves de l'exactitude desboucles **while** seront décrites. Développer une règle d'inférence pour segments de programme du type

en *condition*
    S

notez que S est exécuté à plusieurs reprises jusqu'à ce que la *condition* devienne fausse. Une affirmation qui reste vraie chaque fois que S est exécuté doit être choisi. Une telle assertion est appelée **invariant de boucle**. En d'autre mots, p est un invariant de boucle si *(condition* p ∧ *)* $\{S\}$ p est vrai.

Supposons que p est un invariant de boucle. Il s'ensuit que si p est vrai avant que le segment de programme soit exécutée, les *conditions* p et ¬sont vraies après la résiliation, si elles se produisent. Cette règle d'inférence est

(condition p ∧ *)* $\{S\}$ p

$\therefore p$ { **tandis que la** *condition* S } *(* ¬ *condition* ∧ *p).*

L'utilisation d'un invariant de boucle est illustrée dans l'exemple 4.

EXEMPLE 4 Un invariant de boucle est nécessaire pour vérifier que le segment de programme

$i := 1$
factorielle $:= 1$
alors que *je* $< n$
    $i := i + 1$
    factorielle := *factorielle* $\cdot\ i$

se termine par *factorielle* $= n$! lorsque n est un entier positif.

Soit p l'assertion « $factorielle = i\,!$ et $i \leq n$. »Nous prouvons d'abord que p est un invariant de boucle. Supposons que, au début d'une exécution de la **tandis que** la boucle, p est vrai et l'état de le **tout** en boucle détient; en d'autres termes, supposons que $factorielle = i\,!$ et que $je < n$. Les nouvelles valeurs $i_{nouveau}$ et $factoriel_{nouveau}$ de i et $factoriel$ sont $i_{nouveau} = i + 1$ et $factoriel_{nouveau} = factoriel \cdot (i + 1) = (i + 1)\,! = je_{nouveau}\,!$. Parce que $i < n$, nous avons aussi $i_{new} = i + 1 \leq n$. Ainsi, p est vrai à la fin de l'exécution de la boucle. Cela montre que p est un invariant de boucle.

Nous considérons maintenant le segment du programme. Juste avant d'entrer dans la boucle, $i = 1 \leq n$ et $factorielle = 1 = 1! = i\,!$ les deux tiennent, donc p est vrai. Parce que p est un invariant de boucle, la règle d'inférence rence vient de présenter implicitement que si le **tout** se termine en boucle, il se termine avec p vrai et $i < n$ false. Dans ce cas, à la fin, $factorielle = i\,!$ et $i \leq n$ sont vrais, mais $i < n$ est faux; en d'autre mots, $i = n$ et $factorielle = i\,! = n\,!$, comme souhaité.

Enfin, nous devons vérifier que le **tout** en boucle se termine en fait. Au début de la programmer i reçoit la valeur 1, donc après n - 1 traversals de la boucle, la nouvelle valeur de i volonté être n , et la boucle se termine à ce point. ▲

Un dernier exemple sera donné pour montrer comment les différentes règles d'inférence peuvent être utilisées pour vérifier l'exactitude d'un programme plus long.

EXEMPLE 5 Nous décrirons comment vérifier l'exactitude du programme S pour calculer le produit de deux entiers.

multiplier la **procédure** (m, n : entiers)

S_1 { **si** $n < 0$ **alors** $a := -n$
  sinon $a := n$

S_2 { $k := 0$
  $x := 0$

S_3 { **tandis que** $k < a$
  $x := x + m$
  $k := k + 1$

S_4 { **si** $n < 0$ **alors** $produit := -x$
  sinon $produit := x$

retourner le *produit*
{le *produit* est égal à mn }

Le but est de prouver qu'après l'exécution de S , le *produit* a la valeur mn . La preuve d'exactitude peut être réalisée en divisant S en quatre segments, avec $S = S_1 ; S_2 ; S_3 ; S_4$, comme illustré dans la liste de S . La règle de composition peut être utilisée pour construire la preuve d'exactitude. Voici comment le l'argument se poursuit. Les détails seront laissés en exercice au lecteur.

Soit p l'affirmation initiale « m et n sont des entiers». Ensuite, on peut montrer que $p\ \{S_1\}\ q$ est vrai, lorsque q est la proposition $p \wedge (a = |n|)$. Soit ensuite r la proposition $q \wedge (k = 0) \wedge (x = 0)$. Il on vérifie facilement que $q\ \{S_2\}\ r$ est vrai. On peut montrer que « $x = mk$ et $k \leq a$ » est un invariant pour la boucle dans S_3 . De plus, il est facile de voir que la boucle se termine après *une* itération, avec $k = a$, donc $x = ma$ à ce stade. Parce que r implique que $x = m \cdot 0$ et $0 \leq a$, l'invariant de boucle est vrai avant que la boucle ne soit entrée. Parce que la boucle se termine par $k = a$, il s'ensuit que $r\ \{S_3\}\ s$ est vrai où s est la proposition « $x = ma$ et $a = |n|$. »Enfin, on peut montrer que S_4 est correct avec par rapport à l'assertion initiale s et à l'assertion finale t , où t est la proposition « $produit = mn$ ».

En mettant tout cela ensemble, parce que $p\ \{S_1\}\ q$, $q\ \{S_2\}\ r$, $r\ \{S_3\}\ s$ et $s\ \{S_4\}\ t$ sont tous vrais, cela suit bas de la règle de composition que $p\ \{S\}\ t$ est vrai. De plus, parce que les quatre segments terminer, S *se* termine. Cela vérifie l'exactitude du programme. ▲

Des exercices

1. Montrer que le segment de programme

$y := 1$
$z := x + y$

est correcte par rapport à l'assertion initiale $x = 0$ et l'assertion finale $z = 1$.

2. Vérifiez que le segment de programme

si $x < 0$ **alors** $x := 0$

est correcte en ce qui concerne l'assertion initiale **T** et la assertion finale $x \geq 0$.

3. Vérifiez que le segment de programme

$x := 2$
$z := x + y$
si $y > 0$ **alors**
  $z := z + 1$
autre
  $z := 0$

est correcte par rapport à l'assertion initiale $y = 3$ et l'assertion finale $z = 6$.

4. Vérifiez que le segment de programme

si $x < y$ **alors**
  $min := x$
autre
  $min := y$

est correcte en ce qui concerne l'assertion initiale **T** et la assertion finale $(x \leq y \wedge min = x) \vee (x > y \wedge min = y)$.

∗ **5.** Élaborer une règle d'inférence pour la vérification de la correspondance partielle

rectitude des déclarations du formulaire

si *condition* 1 **alors**
  S_1
sinon si la *condition* 2 **alors**
  S_2
   ...
autre
  S_n

où $S_1, S_2, \ldots, S_n$ sont des blocs.

6. Utilisez la règle d'inférence développée dans l'exercice 5 pour vérifier que le programme

si $x < 0$ **alors**
  $y := -2 |x| / X$
sinon si $x > 0$ **alors**
  $y := 2 |x| / X$
sinon si $x = 0$ **alors**
  $y := 2$

est correcte en ce qui concerne l'assertion initiale **T** et la assertion finale $y = 2$.

7. Utilisez un invariant de boucle pour prouver que le programme suivant segment pour le calcul de la n e puissance, où n est une position entier positif, d'un nombre réel x est correct.

puissance $:= 1$
$i := 1$
tandis que $i \leq n$
  puissance $:=$ *puissance* $* x$
  $i := i + 1$

∗ **8.** Démontrer que le programme itératif de recherche de f_n donné dans

La section 5.4 est correcte.

9. Fournissez tous les détails dans la preuve d'exactitude Exemple 5.

10. Supposons que l'instruction conditionnelle $p_0 \rightarrow p_1$ et l'assertion de programme $p_1 \{ S \} q$ est vraie. Montrer que $p_0 \{ S \} q$ doit également être vrai.

11. Supposons que l'assertion de programme $p \{ S \} q_0$ et l'instruction conditionnelle $q_0 \rightarrow q_1$ est vraie. Montre CA $p \{ S \} q_1$ doit également être vrai.

12. Ce programme calcule les quotients et les restes.

$r := a$
$q := 0$
tandis que $r \geq d$
  $r := r - d$
  $q := q + 1$

Vérifiez qu'il est partiellement correct par rapport à l'ini- l'affirmation fondamentale « a et d sont des entiers positifs» et la assertion « q et r sont des entiers tels que $a = dq + r$ et $0 \leq r < d$. "

13. Utilisez un invariant de boucle pour vérifier que l'algorithme euclidien (Algorithme 1 de la section 4.3) est partiellement correct avec spect à l'affirmation initiale " a et b sont des entiers positifs" et l'assertion finale " $x = \text{pgcd}(a, b)$ ".

Termes et résultats clés

TERMES

séquence: une fonction avec domaine qui est un sous-ensemble de l'ensemble de entiers

progression géométrique: une séquence de la forme $a, ar, ar^2, \ldots$, où a et r sont des nombres réels

progression arithmétique: une séquence de la forme $a, a + d, a + 2d, \ldots$, où a et d sont des nombres réels

le principe de l'induction mathématique: l'énoncé $\forall n P(n)$ est vrai si $P(1)$ est vrai et $\forall k [P(k) \rightarrow P(k+1)]$ est vrai.

étape de base: la preuve de $P(1)$ dans une preuve par in- duction de $\forall n P(n)$

pas inductif: la preuve de $P(k) \rightarrow P(k+1)$ pour toutes les pos- nombres entiers k dans une preuve par induction mathématique de $\forall n P(n)$

forte induction: l'énoncé $\forall nP(n)$ est vrai si $P(1)$ est vrai et $\forall k\,[(P(1) \wedge \cdots \wedge P(k)) \rightarrow P(k+1)]$ est vrai

propriété bien ordonnée: chaque ensemble non vide de négatif les entiers ont un moindre élément.

définition récursive d'une fonction: une définition d'une fonction qui spécifie un ensemble initial de valeurs et une règle pour obtenir les valeurs de cette fonction à des nombres entiers à partir de ses valeurs à plus petit entiers

définition récursive d'un ensemble: une définition d'un ensemble qui spécifie un ensemble initial d'éléments dans l'ensemble et une règle d'obtention d'autres éléments de ceux de l'ensemble

induction structurelle: une technique pour prouver les résultats ensembles définis récursivement

algorithme récursif: un algorithme qui procède en réduisant un problème au même problème avec une entrée plus petite

merge sort: un algorithme de tri qui trie une liste en la divisant en deux, en triant chacune des deux listes résultantes et en fusionnant les résultats dans une liste triée

itération: une procédure basée sur l'utilisation répétée d'opérations en boucle

exactitude du programme: vérification qu'une procédure est toujours produit le résultat correct

invariant de boucle: une propriété qui reste vraie à chaque traversée d'une boucle

assertion initiale: l'instruction spécifiant les propriétés du valeurs d'entrée d'un programme

assertion finale: la déclaration précisant les propriétés de mettre des valeurs devraient avoir si le programme fonctionnait correctement

Questions de révision

1. a) Pouvez-vous utiliser le principe de l'induction mathématique pour trouver une formule pour la somme des n premiers termes d'un séquence?

b) Pouvez-vous utiliser le principe de l'induction mathématique pour déterminer si une formule donnée pour la somme de les n premiers termes d'une séquence sont corrects?

c) Trouver une formule pour la somme des n premiers même positifs entiers, et le prouver en utilisant l'induction mathématique.

2. a) Pour lesquels les entiers positifs n sont $11n + 17 \leq 2^n$?

b) Prouve la conjecture que tu as faite dans la partie (a) en utilisant induction ématique.

3. a) Quels montants d'affranchissement peuvent être formés en utilisant uniquement Timbres de 5 et 9 cents?

b) Prouve la conjecture que tu as faite en utilisant des mathématiques induction.

c) Prouve la conjecture que tu as faite en utilisant une forte induction.

d) Trouvez une preuve de votre conjecture différente de celles vous avez cédé (b) et (c).

4. Donnez deux exemples différents de preuves qui utilisent des duction.

5. a) Indiquez la propriété bien ordonnée pour l'ensemble des entiers.

b) Utilisez cette propriété pour montrer que chaque plus grand peut être écrit comme le produit de nombres premiers.

6. a) Explique pourquoi une fonction f de l'ensemble des integers à l'ensemble des nombres réels est bien défini s'il est défini récursivement en spécifiant $f(1)$ et une règle pour trouver $f(n)$ à partir de $f(n-1)$.

b) Fournir une définition récursive de la fonction $f(n) = (n+1)!$.

7. a) Donnez une définition récursive des nombres de Fibonacci.

b) Montrer que $f_n > \alpha^{n-2}$ chaque fois que $n \geq 3$, où f_n est le n ème terme de la séquence de Fibonacci et $\alpha = (1 + \sqrt{5})/2$.

8. a) Expliquez pourquoi une séquence a_n est bien définie si elle est déamendée récursivement en spécifiant un_1 et un_2 et une règle pour trouver un_n à partir d' $un_1, un_2, \ldots, a_{n-1}$ pour $n = 3, 4, 5, \ldots$.

b) Trouvez la valeur de a_n si $a_1 = 1$, $a_2 = 2$ et $a_n = a_{n-1} + a_{n-2} + \cdots + a_1$, pour $n = 3, 4, 5, \ldots$.

9. Donnez deux exemples de la façon dont les formules bien formées sont une amende récursive pour différents ensembles d'éléments et ators.

10. a) Donnez une définition récursive de la longueur d'une chaîne.

b) Utilisez la définition récursive de la partie (a) et induction structurelle pour prouver que $l(xy) = l(x) + l(y)$.

11. a) Qu'est-ce qu'un algorithme récursif?

b) Décrire un algorithme récursif pour calculer la somme de n nombres dans une séquence.

12. Décrire un algorithme récursif pour calculer le plus grand diviseur commun de deux entiers positifs.

13. a) Décrivez l'algorithme de tri par fusion.

b) Utilisez l'algorithme de tri par fusion pour mettre la liste 4, 10, 1, 5, 3, 8, 7, 2, 6, 9 dans l'ordre croissant.

c) Donnez une estimation de grand O pour le nombre de comparaisons utilisé par le tri par fusion.

14. a) Teste-t-on un programme informatique pour voir s'il produit la sortie correcte pour certaines valeurs d'entrée vérifier que le programme produit toujours la bonne production?

b) Est-ce que montrer qu'un programme informatique est partiellement correcte par rapport à une affirmation initiale et une finale vérifier que le programme produit toujours le sortie correcte? Sinon, que faut-il d'autre?

15. Quelles techniques pouvez-vous utiliser pour montrer qu'un ordinateur long programme est partiellement correct par rapport à une sertion et une affirmation finale?

16. Qu'est-ce qu'une boucle invariante? Comment utilise-t-on un invariant de boucle?

Exercices supplémentaires

1. Utilisez l'induction mathématique pour montrer que $\frac{2}{3} + \frac{2}{9} + \frac{2}{27} + \cdots + \frac{2}{3^n} = 1 - \frac{1}{3^n}$ chaque fois que n est un entier positif.

2. Utilisez l'induction mathématique pour montrer que $1^3 + 3^3 + 5^3 + \cdots + (2n+1)^3 = (n+1)^2(2n^2+4n+1)$ chaque fois que n est un entier positif.

3. Utilisez l'induction mathématique pour montrer que $1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = (n-1) \cdot 2^n + 1$ chaque fois que n est un entier positif.

4. Utilisez l'induction mathématique pour montrer que

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

chaque fois que n est un entier positif.

5. Montrez que

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \cdots + \frac{1}{(3n-2)(3n+1)} = \frac{n}{3n+1}$$

chaque fois que n est un entier positif.

6. Utilisez l'induction mathématique pour montrer que $2^n > n^2 + n$ chaque fois que n est un entier supérieur à 4.

7. Utilisez l'induction mathématique pour montrer que $2^n > n^3$ quand-toujours n est un entier supérieur à 9.

8. Trouvez un entier N tel que $2^n > n^4$ chaque fois que n est supérieur de N. Démontrez que votre résultat est correct en utilisant induction thermique.

9. Utiliser l'induction mathématique pour prouver que $a - b$ est un facteur d' $un^n - b^n$ chaque fois que n est un entier positif.

10. Utiliser l'induction mathématique pour prouver que 9 divise $n^3 + (n+1)^3 + (n+2)^3$ chaque fois que n est un entier non négatif.

11. Utilisez l'induction mathématique pour prouver que 43 divisions $6^{n+1} + 7^{2n-1}$ pour chaque entier positif n.

12. Utilisez l'induction mathématique pour prouver que 64 divisions $3^{2n+2} + 56n + 55$ pour chaque entier positif n.

13. Utilisez l'induction mathématique pour prouver cette formule somme des termes d'une progression arithmétique.

$$a + (a+d) + \cdots + (a+nd) = (n+1)(2a+nd)/2$$

14. Supposons que $a_j \equiv b_j \pmod m$ pour $j = 1, 2, \ldots, n$. Utilisation induction mathématique pour prouver que

une) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod m$.

b) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod m$.

15. Montrer que si n est un entier positif, alors

$$\sum_{k=1}^{n} \frac{k+4}{k(k+1)(k+2)} = \frac{n(3n+7)}{2(n+1)(n+2)}.$$

16. Pour quels entiers positifs n est $n + 6 < (n^2 - 8n)/16$? Prouvez votre réponse en utilisant l'induction mathématique.

17. (*Nécessite un calcul*) Supposons que $f(x) = e^x$ et $g(x) = xe^x$. Utilisez l'induction mathématique avec le produit règle uct et le fait que $f'(x) = e^x$ prouver que $g^{(n)}(x) = (x+n)e^x$ chaque fois que n est un entier positif.

18. (*Nécessite un calcul*) Supposons que $f(x) = e^x$ et $g(x) = e^{cx}$, où c est une constante. Utilisez l'induction mathématique pour-gether avec la règle de la chaîne et le fait que $f'(x) = e^x$ à prouver que $g^{(n)} = c^n e^{cx}$ chaque fois que n est un entier positif.

∗ **19.** Formuler une conjecture sur laquelle les nombres de Fibonacci sont pairs et utilisent une forme d'induction mathématique pour prouver votre conjecture.

∗ **20.** Déterminez quels nombres de Fibonacci sont divisibles par 3. Utilisez une forme d'induction mathématique pour prouver votre jecture.

∗ **21.** Démontrer que $f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1}$ pour tous les nonnega-entiers n et k, où f_i désigne le i ème Fibonacci nombre.

Rappelons de l'exemple 15 de la section 2.4 que la séquence des **nombres** de **Lucas** est défini par $l_0 = 2$, $l_1 = 1$ et $l_n = l_{n-1} + l_{n-2}$ pour $n = 2, 3, 4, \ldots$.

22. Montrer que $f_n + f_{n+2} = l_{n+1}$ chaque fois que n est un teger, où f_i et l_i sont le i ème nombre de Fibonacci et i e nombre de Lucas, respectivement.

23. Montrer que $l_0^2 + l_1^2 + \cdots + l_n^2 = l_n l_{n+1} + 2$ chaque fois que n est un entier non négatif et l_i est le i ème nombre de Lucas.

∗ **24.** Utiliser l'induction mathématique pour montrer que le produit de tout n entier positif consécutif est divisible par $n!$. [*Astuce:* utiliser le identité $m(m+1)\cdots(m+n-1)/n! = (m-1)m(m+1)\cdots(m+n-2)/n! + m(m+1)\cdots(m+n-2)/(n-1)!$.]

25. Utiliser l'induction mathématique pour montrer que $(\cos x + i \sin x)^n = \cos nx + i \sin nx$ chaque fois que n est un positif Teger. (Ici, *je suis* la racine carrée de -1.) [*Astuce:* Utiliser les identités $\cos(a+b) = \cos a \cos b - \sin a \sin b$ et $\sin(a+b) = \sin a \cos b + \cos a \sin b$.]

∗ **26.** Utilisez l'induction mathématique pour montrer que $\sum_{j=1}^{n} \cos jx = \cos[(n+1)x/2] \sin(nx/2)/\sin(x/2)$ chaque fois que n est un entier positif et $\sin(x/2) = 0$.

27. Utiliser l'induction mathématique pour prouver que $\sum_{j=1}^{n} j^2 2^j = n^2 2^{n+1} - n 2^{n+2} + 3 \cdot 2^{n+1} - 6$ pour chaque entier positif ger n.

28. (*Nécessite un calcul*) Supposons que la séquence $x_1, x_2, \ldots, x_n, \ldots$ est récursivement défini par $x_1 = 0$ et $x_{n+1} = \sqrt{x_n + 6}$.

a) Utiliser l'induction mathématique pour montrer que $x_1 < x_2 < \cdots < x_n < \cdots$, c'est-à-dire que la séquence $\{x_n\}$ est monotone-en augmentation.

b) Utiliser l'induction mathématique pour prouver que $x_n < 3$ pour $n = 1, 2, \ldots$.

c) Montrer que $\lim_{n \to \infty} x_n = 3$.

29. Montrer si n est un entier positif avec $n \geq 2$, alors

$$\sum_{j=2}^{n} \frac{1}{j^2 - 1} = \frac{(n-1)(3n+2)}{4n(n+1)}.$$

30. Utilisez l'induction mathématique pour prouver le théorème 1 tion 4.2, c'est-à-dire montrer si b est un entier, où $b > 1$, et n est un entier positif, alors n peut être exprimé uniquement sous la forme $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$.

∗ **31.** Un **point de réseau** dans le plan est un point (x, y) où les deux x et y sont des entiers. Utilisez l'induction mathématique pour montrer qu'au moins $n + 1$ lignes droites sont nécessaires pour garantir que chaque point du réseau (x, y) avec $x \geq 0$, $y \geq 0$, et $x + y \leq n$ se trouve sur l'une de ces lignes.

32. (*Nécessite un calcul*) Utilisez l'induction mathématique et le règle de produit pour montrer que si n est un entier positif et $f_1(x), f_2(x), \ldots, f_n(x)$, sont toutes des fonctions différenciables, ensuite

$$\frac{(f_1(x) f_2(x) \cdots f_n(x))'}{f_1(x) f_2(x) \cdots f_n(x)}$$

groupe qui peut effectuer un tour en obtenant du gaz d'autres voitures comme il se déplace autour de la piste.

41. Montrer que si n est un entier positif, alors

$$\sum_{j=1}^{n} (2j-1) \left(\sum_{k=j}^{n} 1/k \right) = n(n+1)/2.$$

42. Utilisez l'induction mathématique pour montrer que si a, b et c sont les longueurs des côtés d'un triangle rectangle, où c est la longueur de l'hypoténuse, puis $a^n + b^n < c^n$ pour tous entiers n avec $n \geq 3$.

∗ **43.** Utilisez l'induction mathématique pour montrer que si n est un entiers positifs, la séquence $2 \ \mathbf{mod}\ n$, $2^2 \ \mathbf{mod}\ n$, $2^{2^2} \ \mathbf{mod}\ n$, $2^{2^{2^2}} \ \mathbf{mod}\ n, \ldots$ est finalement constant (c'est-à-dire tous les termes

$$= \frac{f_1(x)}{f_1(x)} + \frac{f_2(x)}{f_2(x)} + \cdots + \frac{f_n(x)}{f_n(x)}.$$

33. (*Requiert des éléments de la section 2.6*) Supposons que $\mathbf{B} = \mathbf{MAM}^{-1}$, où **A** et **B** sont $n \times n$ matrices et **M** est inversible. Montrez que $\mathbf{B}^k = \mathbf{MA}^k\mathbf{M}^{-1}$ pour tous les tegers k . (Consultez à la fois le texte de la section 2.6 et le préambule de l'exercice 18 de la section 2.6.)

34. Utilisez l'induction mathématique pour montrer que si vous dessinez des lignes dans l'avion il suffit de deux couleurs pour colorer les régions formées de façon à ce qu'il n'existe pas deux régions mon ont une couleur commune.

35. Montrez que n ! peut être représenté comme la somme de n de ses des diviseurs positifs distincts chaque fois que $n \geq 3$. [*Indice:* utilisez charge ductive. Essayez d'abord de prouver ce résultat en utilisant induction matique. En examinant où votre preuve échoue, trouver une déclaration plus forte que vous pouvez facilement prouver en utilisant Induction mathematique.]

∗ **36.** Utiliser l'induction mathématique pour prouver que si $x_1, x_2, \ldots, x_n$ sont des nombres réels positifs avec $n \geq 2$, alors

$$\left(x_1 + \frac{1}{x_1}\right)\left(x_2 + \frac{1}{x_2}\right) \cdots \left(x_n + \frac{1}{x_n}\right) \geq \left(x_1 + \frac{1}{x_2}\right)\left(x_2 + \frac{1}{x_3}\right) \cdots \left(x_{n-1} + \frac{1}{x_n}\right)\left(x_n + \frac{1}{x_1}\right)$$

37. Utiliser l'induction mathématique pour prouver que si n personnes se tiennent dans une ligne, où n est un entier positif, et si la première per- fils dans la ligne est une femme et la dernière personne en ligne est un l'homme, puis quelque part dans la ligne, il y a une femme directement devant un homme.

∗ **38.** Supposons que pour chaque paire de villes d'un pays, il existe un route à sens unique directe les reliant dans une direction ou L'autre. Utiliser l'induction mathématique pour montrer qu'il est une ville accessible depuis toutes les autres villes directement ou via exactement une autre ville.

39. Utiliser l'induction mathématique pour montrer que lorsque n cercles diviser l'avion en régions, ces régions peuvent être col- orné de deux couleurs différentes de sorte qu'aucune région la frontière commune est de la même couleur.

∗ **40.** Supposons que parmi un groupe de voitures sur une piste circulaire il y a suffisamment de carburant pour une voiture pour effectuer un tour. Utilisation induction mathématique pour montrer qu'il y a une voiture dans le

après un nombre fini de termes sont tous les mêmes).

44. Une **unité** ou une **fraction égyptienne** est une fraction de la forme $1/n$, où n est un entier positif. Dans cet exercice, nous utilisera une forte induction pour montrer qu'un algorithme gourmand peut être utilisé pour exprimer chaque nombre rationnel p/q avec $0 < p/q < 1$ comme la somme de fractions unitaires distinctes. À chaque étape de l'algorithme, on trouve le plus petit entier positif n tel que $1/n$ puisse être ajouté à la somme sans dépasser ing p/q . Par exemple, pour Express $5/7$, nous commençons la somme avec $1/2$. Parce que $5/7 - 1/2 = 3/14$ nous ajoutons $1/5$ la somme parce que 5 est le plus petit entier positif k tel que $1/k < 3/14$. Comme $3/14 - 1/5 = 1/70$, l'algo- Rithm se termine, montrant que le $5/7 = 1/2 + 1/5 + 1/70$. Soit $T(p)$ la déclaration que cet algorithme se termine pour tous les nombres rationnels p/q avec $0 < p/q < 1$. Nous allons prouver que l'algorithme se termine toujours en montrant que $T(p)$ vaut pour tous les entiers positifs p .

a) Montrer que l'étape de base $T(1)$ est vérifiée.

b) Supposons que $T(k)$ *soit* vrai pour les entiers positifs k avec $k < p$. Autrement dit, supposons que l'algorithme se termine pour tous les nombres rationnels k/r , où $1 \leq k < p$. Spectacle que si nous commençons par p/q et la fraction $1/n$ est sé- sélectionné dans la première étape de l'algorithme, puis $p/q = p/q + 1/n$, où $p = np - q$ et $q = nq$. Après considérant le cas où $p/q = 1/n$, utilisez l'in- hypothèse ductive pour montrer que l'algorithme gourmand se termine quand il commence par p/q et complète la étape inductive.

La **fonction McCarthy 91** (définie par John McCarthy, un des fondateurs de l'intelligence artificielle) est définie à l'aide règle

$$M(n) = \begin{cases} n - 10 & \text{si } n > 100 \\ M(M(n + 11)) & \text{si } n \leq 100 \end{cases}$$

pour tous les entiers positifs n .

45. En utilisant successivement la règle de définition de $M(n)$, trouver

a) $M(102)$. **b)** $M(101)$. **c)** $M(99)$.
d) $M(97)$. **e)** $M(87)$. **f)** $M(76)$.

∗∗ **46.** Montrer que la fonction $M(n)$ est une fonction bien définie de l'ensemble des entiers positifs à l'ensemble des entiers positifs gers. [*Astuce:* Démontrez que $M(n) = 91$ pour tous les entiers positifs n avec $n \leq 101$.]

47. Est-ce la preuve que

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} = \frac{3}{2} - \frac{1}{n},$$

chaque fois que n est un entier positif, correct? Justifiez votre swer.

Étape de base: le résultat est vrai lorsque $n = 1$ car

$$\frac{1}{1 \cdot 2} = \frac{3}{2} - \frac{1}{1}.$$

Étape inductive: Supposons que le résultat est vrai pour n . alors

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} = \left(\frac{3}{2} - \frac{1}{n}\right) + \frac{1}{n} - \frac{1}{n+1} = \frac{3}{2} - \frac{1}{n+1}.$$

Par conséquent, le résultat est vrai pour $n + 1$ s'il est vrai pour n . Cette complète la preuve.

48. Supposons que $A_1, A_2, \ldots, A_n$ sont une collection d'ensembles. Supposons que $R_2 = A_1 \oplus A_2$ et $R_k = R_{k-1} \oplus A_k$ pour $k = 3, 4, \ldots, n$. Utilisez l'induction mathématique pour prouver que $x \in R_n$ si et seulement si x appartient à un nombre impair de définit $A_1, A_2, \ldots, A_n$. (Rappelons que $S \oplus T$ est le symétrique différence des ensembles S et T définis dans le préambule de Exercice 32 de la section 2.2.)

∗ **49.** Montrer que n cercles divisent le plan en $n^2 - n + 2$ re si tous les deux cercles se croisent en exactement deux points

élément a . Ensuite , montrer que $la\sqrt{2} - a$ est un plus petit positif entier de cette forme.]

52. Un ensemble est **bien ordonné** si chaque sous-ensemble non vide de ce set a un moindre élément. Déterminez si chacun des les ensembles suivants sont bien ordonnés.

a) l'ensemble des entiers

b) l'ensemble des entiers supérieur à −100

c) l'ensemble des logiques positives

d) l'ensemble des justifications positives dont le dénominateur est inférieur à 100

53. a) Montrer que si $a_1, a_2, \ldots, a_n$ sont des entiers positifs, alors gcd $(a_1, a_2, \ldots, a_{n-1}, a_n)$ = gcd $(a_1, a_2, \ldots, a_{n-2}$, pgcd $(a_{n-1}, a_n))$.

b) Utiliser la partie (a), avec l'algorithme euclidien, pour développer un algorithme récursif pour calculer les est le diviseur commun d'un ensemble de n entiers positifs.

∗ **54.** Décrire un algorithme récursif pour écrire le plus grand diviseur commun de n entiers positifs en combinaison linéaire nation de ces nombres entiers.

55. Trouvez une formule explicite pour $f(n)$ si $f(1) = 1$ et $f(n) = f(n-1) + 2n - 1$ pour $n \geq 2$. Prouvez votre résultat en utilisant Induction mathematique.

∗∗ **56.** Donner une définition récursive de l'ensemble de chaînes de bits contiennent deux fois plus de 0 que de 1.

57. Soit S l'ensemble des chaînes de bits définies récursivement par $\lambda \in S$ et $0x \in S$, $x1 \in S$ si $x \in S$, où λ est la chaîne vide.

a) Trouvez toutes les chaînes en S d'une longueur ne dépassant pas cinq.

b) Donner une description explicite des éléments de S .

et pas trois cercles contiennent un point commun.

∗ **50.** Montrer que n plans divisent l'espace tridimensionnel en $(n^3 + 5n + 6)/6$ régions si trois de ces avions ont exactement un point en commun et aucun ne contient un commun point.

∗ **51.** Utilisez la propriété bien ordonnée pour montrer que $\sqrt{2}$ est irrationnel. [*Astuce:* Supposons que $\sqrt{2}$ est rationnel. Montre CA l'ensemble des entiers positifs de la forme $b\sqrt{2}$ a au moins

58. Soit S l'ensemble des chaînes définies récursivement par $abc \in S$, $bac \in S$ et $acb \in S$, où a, b et c sont des lettres fixes; et pour tout $x \in S$, $abcx \in S$; $abxc \in S$, $axbc \in S$ et $xabc \in S$, où x est une variable représentant une chaîne de des lettres.

a) Trouvez tous les éléments de S de longueur huit ou moins.

b) Montrer que chaque élément de S a une longueur divisible par Trois.

JOHN McCARTHY (NÉ EN 1927) John McCarthy est né à Boston. Il a grandi à Boston et à Los Angeles. Il a étudié les mathématiques en tant qu'étudiant de premier cycle et étudiant diplômé, recevant son BS en 1948 de le California Institute of Technology et son doctorat. en 1951 de Princeton. Après avoir été diplômé de Princeton, McCarthy a occupé des postes à Princeton, Stanford, Dartmouth et MIT Il a occupé un poste à Stanford à partir de 1962 jusqu'en 1994, et y est maintenant professeur émérite. À Stanford, il était directeur de l'intelligence artificielle Laboratoire, détenait une chaire nommée à la School of Engineering, et était chercheur principal à la Hoover Institution.

McCarthy a été un pionnier dans l'étude de l'intelligence artificielle, un terme qu'il a inventé en 1955. Il a travaillé sur les problèmes liés aux besoins de raisonnement et d'information requis pour un comportement informatique intelligent. McCarthy a été parmi les premiers informaticiens à concevoir des systèmes informatiques à temps partagé. Il a développé LISP, un langage de programmation pour l'informatique utilisant des expressions symboliques. Il a joué un rôle important dans l'utilisation de la logique pour vérifier l'exactitude des programmes informatiques. McCarthy a également travaillé sur les implications sociales de la technologie informatique. Il travaille actuellement sur le problème de la façon dont les gens et les ordinateurs font des conjectures en supposant que les complications sont absentes des situations. McCarthy est un défenseur de la durabilité du progrès humain et un optimiste quant à l'avenir de l'humanité. Il a également commencé écrire des histoires de science-fiction. Certains de ses écrits récents explorent la possibilité que le monde soit un programme informatique écrit par une force plus élevée.

McCarthy a notamment remporté le prix Turing de l'Association for Computing Machinery, le Research Prix d'excellence de la Conférence internationale sur l'intelligence artificielle, le prix de Kyoto et la médaille nationale des sciences.

L'ensemble B de toutes les **chaînes de parenthèses équilibrées** est défini récursivement par $\lambda \in B$, où λ est la chaîne vide; $(x) \in B$, $xy \in B$ si $x, y \in B$.

59. Montrez que $(()\,())$ est une chaîne équilibrée de parenthèses et $(()))$ n'est pas une chaîne équilibrée de parenthèses.

60. Trouvez toutes les chaînes de parenthèses équilibrées avec exactement six symboles.

61. Trouver toutes les chaînes équilibrées de parenthèses avec quatre ou moins symboles.

62. Utilisez l'induction pour montrer que si x est une chaîne équilibrée de parenthèses, le nombre de parenthèses gauches est égal à le nombre de parenthèses droites en x.

Définissez la fonction N sur l'ensemble des chaînes de parenthèses par

$$N(\lambda) = 0,\ N(() = 1,\ N()) = -1,$$
$$N(uv) = N(u) + N(v),$$

où λ est la chaîne vide et u et v sont des chaînes. Ça peut être a montré que N est bien défini.

63. Trouver

a) $N(())$. **b)** $N()))\,())\,(()$.

c) $N(((()\,(())$. **d)** $N(()\,((()))\,(()))$.

∗∗ **64.** Montrer qu'une chaîne w de parenthèses est équilibrée si et seulement si $N(w) = 0$ et $N(u) \geq 0$ chaque fois que u est un préfixe de w, c'est-à-dire $w = uv$.

∗ **65.** Donner un algorithme récursif pour trouver toutes les chaînes équilibrées de parenthèses contenant n ou moins de symboles.

66. Donner un algorithme récursif pour trouver le pgcd (a, b), où a et b sont des entiers non négatifs non tous deux nuls, sur la base de ces faits: gcd $(a, b) =$ gcd (b, a) si $a > b$, pgcd $(0, b) = b$, pgcd $(a, b) = 2$ pgcd $(a/2, b/2)$ si a et b sont pair, gcd $(a, b) =$ gcd $(a/2, b)$ si a est pair et b est impair, et pgcd $(a, b) =$ pgcd $(a, b - a)$.

67. Vérifiez le segment de programme

si $x > y$ **alors**
$x := y$

par rapport à l'assertion initiale **T** et à l' assertion finale tion $x \leq y$.

∗ **68.** Élaborer une règle d'inférence pour vérifier les programmes récursifs grammes et l'utiliser pour vérifier l'algorithme récursif pour la commettre les factoriels donnés comme algorithme 1 dans la section 5.4.

Projets informatiques

69. Concevoir un algorithme récursif qui compte le nombre de fois l'entier 0 apparaît dans une liste d'entiers.

Les exercices 70 à 77 traitent de séquences inhabituelles, formellement appelées **séquences auto-génératrices**, produites par relations ou règles de récurrence simples. En particulier, Exercices 70 à 75 traitent de la séquence $\{a(n)\}$ définie par $a(n) = n - a(a(n-1))$ pour $n \geq 1$ et $a(0) = 0$. (Cette séquence ainsi que celles des exercices 74 et 75 sont définies dans le fascinant livre de Douglas Hofstader *Gödel, Escher, Bach* ([Ho99]).

70. Trouvez les 10 premiers termes de la séquence $\{a(n)\}$ définie dans le préambule de cet exercice.

∗ **71.** Prouver que cette séquence est bien définie. Autrement dit, montrer que $a(n)$ est défini de manière unique pour tous les entiers non négatifs n.

∗∗ **72.** Démontrer que $a(n) = \lfloor (n+1)\mu \rfloor$ où $\mu = (-1 + \sqrt{5})/2$.

[*Astuce:* Premier spectacle pour tout $n > 0$ que $(\mu n - \lfloor \mu n \rfloor) + (\mu^2 n - \lfloor \mu^2 n \rfloor) = 1$. Ensuite, montrez pour tous les nombres réels α avec $0 \leq \alpha < 1$ et $\alpha = 1 - \mu$ que $\lfloor (1+\mu)(1-\alpha) \rfloor + \lfloor \alpha + \mu \rfloor = 1$, en considérant les cas $0 \leq \alpha < 1 - \mu$ et $1 - \mu < \alpha < 1$ séparément.]

∗ **73.** Utilisez la formule de l'exercice 72 pour montrer que $a(n) = a(n-1)$ si $\mu n - \lfloor \mu n \rfloor < 1 - \mu$ et $a(n) = a(n-1) + 1$ sinon.

74. Trouvez les 10 premiers termes de chacun des génération de séquences:

a) $a(n) = n - a(a(a(n-1)))$ pour $n \geq 1$, $a(0) = 0$

b) $a(n) = n - a(a(a(a(n-1))))$ pour $n \geq 1$, $a(0) = 0$

c) $a(n) = a(n - a(n-1)) + a(n - a(n-2))$ pour $n \geq 3$, $a(1) = 1$ et $a(2) = 1$

75. Trouvez les 10 premiers termes des séquences $m(n)$ et $f(n)$ définie par la paire suivante de récurrences entrelacées relations de rence: $m(n) = n - f(m(n-1))$, $f(n) = n - m(f(n-1))$ pour $n \geq 1$, $f(0) = 1$ et $m(0) = 0$.

La séquence autogénératrice de **Golomb** est l'unique séquence croissante des entiers positifs $a_1, a_2, a_3, \ldots$ qui a la propriété qu'il contient exactement une_k occurrences de k pour chaque entier positif k.

76. Trouvez les 20 premiers termes de la génération autogénérée de Golomb. par conséquent.

∗ **77.** Montrer que si $f(n)$ est le plus grand entier m tel que $a_m = n$, où a_m est le m ième terme de Golomb séquence auto-génératrice, alors $f(n) = \sum_{k=1}^{n} a_k$ et $f(f(n)) = \sum_{k=1}^{n} ka_k$.

Écrivez des programmes avec ces entrées et sorties.

∗∗ **1.** Étant donné un $2^n \times 2^n$ damier avec un carré manquant, construire un pavage de ce damier en utilisant le trio droit non.

∗∗ **2.** Générez toutes les formules bien formées pour les expressions faisant tourner les variables x , y et z et les opérateurs $\{+, *, /, -\}$ avec n symboles ou moins.

∗∗ **3.** Générez toutes les formules bien formulées pour les propositions avec n symboles ou moins où chaque symbole est **T** , **F** , l'un des les variables propositionnelles p et q , ou un opérateur de $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$.

4. Étant donné une chaîne, trouvez son inversion.

5. Étant donné un nombre réel a et un entier non négatif n , trouver a^n en utilisant la récursivité.

6. Étant donné un nombre réel a et un entier non négatif n , trouver a^{2^n} en utilisant la récursivité.

∗ **7.** Étant donné un nombre réel a et un entier non négatif n , trouver un^n en utilisant l'expansion binaire de n et un algorithme récursif pour calculer un^{2^k} .

8. Étant donné deux nombres entiers non différents de zéro, trouvez leur plus diviseur mon en utilisant la récursivité.

9. Étant donné une liste d'entiers et d'un élément x , recherchez x dans ce liste utilisant une implémentation récursive d'une recherche linéaire.

10. Étant donné une liste d'entiers et d'un élément x , recherchez x dans ce liste utilisant une implémentation récursive d'une recherche binaire.

11. Étant donné un entier non négatif n , trouver le n ème Fibonacci nombre utilisant l'itération.

12. Étant donné un entier non négatif n , trouver le n ème Fibonacci nombre utilisant la récursivité.

13. Étant donné un entier positif, trouvez le nombre de partitions de cet entier. (Voir l'exercice 47 de la section 5.3.)

14. Étant donné les entiers positifs m et n , trouvez $A(m, n)$, la valeur de Fonction d'Ackermann à la paire (m, n) . (Voir le préambule à l'exercice 48 de la section 5.3.)

15. Étant donné une liste de n entiers, triez ces entiers en utilisant tri par fusion.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Quelles sont les plus grandes valeurs de n pour lesquelles n ! a moins de 100 chiffres décimaux et moins de 1 000 chiffres décimaux?

2. Déterminez quels nombres de Fibonacci sont divisibles par 5, qui sont divisibles par 7, et qui sont divisibles par 11. Prouvez que vos conjectures sont correctes.

3. Construire des pavages en utilisant des triominos droits de 16 × 16 différents, Damiers 32 × 32 et 64 × 64 avec un carré manquant ing.

4. Découvrez quels $m \times n$ damiers peuvent être complètement recouvert de triominos droits. Pouvez-vous faire une conjecture qui répond à cette question?

∗∗ **5.** Mettre en œuvre un algorithme pour déterminer si un point se trouve à l'intérieur ou à l'extérieur d'un simple polygone.

∗∗ **6.** Mettre en œuvre un algorithme pour trianguler un poly- gon.

7. Quelles valeurs de la fonction d'Ackermann sont suffisamment petites que vous êtes capable de les calculer?

8. Comparez le nombre d'opérations ou le temps nécessaire pour calculer les nombres de Fibonacci récursivement par rapport qui devait les calculer de manière itérative.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Décrivez les origines de l'induction mathématique. Qui étaient les premières personnes à l'utiliser et à quels problèmes ont-ils l'appliquer?

2. Expliquez comment prouver le théorème de la courbe de Jordan pour pleins polygones et décrire un algorithme pour déterminer si un point est à l'intérieur ou à l'extérieur d'un simple polygone.

3. Décrire comment la triangulation de polygones simples est utilisée dans certains algorithmes clés en géométrie de calcul.

4. Décrire une variété d'applications différentes du Fibonacci nombres aux sciences biologiques et physiques.

5. Discutez des utilisations de la fonction d'Ackermann dans la théorie des définitions récursives et dans l'analyse de la complexité des algorithmes pour les unions d'ensembles.

6. Discutez de certaines des diverses méthodologies utilisées pour établir l'exactitude des programmes et les comparer à Les méthodes de Hoare décrites dans la section 5.5.

7. Expliquez comment les idées et les concepts de l'exactitude du programme peut être étendu pour prouver que les systèmes d'exploitation sont sécurisés.

CHAPITRE

Compte

La combinatoire, l'étude des agencements d'objets, est une partie importante des mathématiques discrètes. ématiques. Ce sujet a été étudié dès le XVIIe siècle, lorsque la combinaison des questions natoriales se sont posées dans l'étude des jeux de hasard. Dénombrement, comptage d'objets avec certaines propriétés, est une partie importante de la combinatoire. Il faut compter les objets à résoudre de nombreux types de problèmes différents. Par exemple, le comptage est utilisé pour déterminer la complexité de algorithmes. Le décompte est également nécessaire pour déterminer s'il y a suffisamment de numéros de téléphone ou des adresses de protocole Internet pour répondre à la demande. Récemment, il a joué un rôle clé en mathématiques la biologie, en particulier dans le séquençage de l'ADN. De plus, les techniques de comptage sont largement utilisées lorsque les probabilités d'événements sont calculées.

Les règles de base du comptage, que nous étudierons à la section 6.1, peuvent résoudre un énorme variété de problèmes. Par exemple, nous pouvons utiliser ces règles pour énumérer les différents téléphones aux États-Unis, les mots de passe autorisés sur un système informatique et le nombre de différents ordres dans lesquels les coureurs d'une course peuvent terminer. Un autre outil combinatoire important est le principe du pigeonnier, que nous étudierons dans la section 6.2. Cela indique que lorsque les objets sont placés dans des boîtes et il y a plus d'objets que de boîtes, puis il y a une boîte contenant au moins deux objets. Par exemple, nous pouvons utiliser ce principe pour montrer que parmi un ensemble de 15 élèves ou plus, au moins 3 sont nés le même jour de la semaine.

Nous pouvons formuler de nombreux problèmes de comptage en termes d'arrangements ordonnés ou les objets d'un ensemble avec ou sans répétitions. Ces arrangements, appelés permutations et sont utilisées dans de nombreux problèmes de comptage. Par exemple, supposons que les 100 meilleurs finisseurs sur concours, 2000 étudiants sont conviés à un banquet. On peut compter les possibles ensembles de 100 étudiants qui seront invités, ainsi que les façons dont les 10 premiers prix peuvent être décernés décerné.

Un autre problème en combinatoire implique de générer tous les arrangements d'un gentil. Ceci est souvent important dans les simulations informatiques. Nous allons concevoir des algorithmes pour générer arrangements de divers types.

Les bases du comptage

introduction

Supposons qu'un mot de passe sur un système informatique se compose de six, sept ou huit caractèresChaque l'un de ces caractères doit être un chiffre ou une lettre de l'alphabet. Chaque mot de passe doit contenir au moins Un chiffre. Combien de ces mots de passe existe-t-il? Les techniques nécessaires pour répondre à cette question et une grande variété d'autres problèmes de comptage seront introduits dans cette section.

Les problèmes de comptage se posent en mathématiques et en informatique. Par exemple, nous doit compter les résultats positifs des expériences et tous les résultats possibles de ces expériences pour déterminer les probabilités d'événements discrets. Nous devons compter le nombre de opérations utilisées par un algorithme pour étudier sa complexité temporelle.

Nous présenterons les techniques de base du comptage dans cette section. Ces méthodes servent de la base de presque toutes les techniques de comptage.

Principes de base du comptage

Nous présentons d'abord deux principes de comptage de base, la **règle de produit** et la **règle de somme** . Ensuite, nous montrer comment ils peuvent être utilisés pour résoudre de nombreux problèmes de comptage différents.

La règle de produit s'applique lorsqu'une procédure est composée de tâches distinctes.

LA RÈGLE DU PRODUIT Supposons qu'une procédure puisse être décomposée en une séquence de deux tâches. S'il y a n_1 façons de faire la première tâche et pour chacune de ces façons de faire la première tâche, il y a n_2 façons de faire la deuxième tâche, puis il y a $n_1 n_2$ façons de faire la procédure.

Les exemples 1 à 10 montrent comment la règle de produit est utilisée.

EXEMPLE 1 Une nouvelle entreprise avec seulement deux employés, Sanchez et Patel, loue un étage d'un immeuble 12 bureaux. De combien de façons existe-t-il d'affecter différents bureaux à ces deux employés?

Solution: La procédure d'attribution de bureaux à ces deux salariés consiste à attribuer un bureau à Sanchez, ce qui peut être fait de 12 façons, puis attribuer un bureau à Patel différent de le bureau attribué à Sanchez, ce qui peut se faire de 11 façons.Selon la règle du produit, il existe $12 \cdot 11 = 132$ façons d'affecter des bureaux à ces deux employés. ▲

EXEMPLE 2 Les chaises d'un auditorium doivent être étiquetées avec une lettre anglaise majuscule suivie d'un entier positif ne dépassant pas 100. Quel est le plus grand nombre de chaises pouvant être étiquetées différemment?

Solution: la procédure d'étiquetage d'une chaise se compose de deux tâches, à savoir l'attribution au siège l'une des 26 lettres anglaises majuscules, puis en lui affectant l'un des 100 entiers possibles. La règle du produit montre qu'il existe $26 \cdot 100 = 2600$ manières différentes d'étiqueter une chaise. Par conséquent, le plus grand nombre de chaises pouvant être étiquetées différemment est 2600. ▲

EXEMPLE 3 Il y a 32 micro-ordinateurs dans un centre informatique. Chaque micro-ordinateur possède 24 ports. Comment y a-t-il de nombreux ports différents vers un micro-ordinateur au centre?

Solution: la procédure de choix d'un port consiste en deux tâches, en premier lieu le choix d'un micro-ordinateur puis choisir un port sur ce micro-ordinateur. Parce qu'il y a 32 façons de choisir le micro-ordinateur et 24 façons de choisir le port, quel que soit le micro-ordinateur sélectionné, la règle du produit montre qu'il y a $32 \cdot 24 = 768$ ports. ▲

Une version étendue de la règle du produit est souvent utile.Supposons qu'une procédure soit exécutée en effectuant les tâches $T_1, T_2, ..., T_m$ en séquence. Si chaque tâche T_i, $i = 1, 2, ..., n$, peut être effectué de n_i façons, quelle que soit la façon dont les tâches précédentes ont été effectuées, il existe alors $n_1 \cdot n_2 \cdot \cdots \cdot n_m$ façons de mener à bien la procédure.Cette version de la règle du produit peut être prouvée par des induction de la règle du produit pour deux tâches (voir exercice 72).

EXEMPLE 4 Combien y a-t-il de chaînes de bits différentes de longueur sept?

Solution: Chacun des sept bits peut être choisi de deux manières, car chaque bit est soit 0 soit 1. Par conséquent, la règle de produit indique qu'il existe un total de $2^7 = 128$ chaînes de bits différentes de longueur Sept. ▲

EXEMPLE 5 Combien de plaques d'immatriculation différentes peuvent être faites si chaque plaque contient une séquence de trois lettres anglaises majuscules suivies de trois chiffres (et aucune séquence de lettres n'est interdite, même s'ils sont obscènes)?

26 choix pour chaque lettre 10 choix pour chaque chiffre

Solution: il y a 26 choix pour chacune des trois lettres anglaises majuscules et dix choix pour chacun des trois chiffres. Par conséquent, selon la règle du produit, il y a un total de $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 =$ 17 , 576 , 000 plaques d'immatriculation possibles. ▲

EXEMPLE 6 **Fonctions de comptage** Combien de fonctions y a-t-il d'un ensemble avec m éléments à un ensemble avec n éléments?

Solution: Une fonction correspond à un choix d'un des n éléments du codomaine pour chacun des les m éléments du domaine. Par conséquent, selon la règle du produit, il y a $n \cdot n \cdot \cdots \cdot n = n^m$ les fonctions d'un ensemble avec m éléments à un avec n éléments. Par exemple, il y a $5^3 = 125$ différents fonctions d'un ensemble à trois éléments à un ensemble à cinq éléments. ▲

EXEMPLE 7 **Comptage des fonctions un-à-un** Combien de **fonctions** un-à-un existe-t-il dans un ensemble avec m éléments à un avec n éléments?

Compter le nombre de sur les fonctions est plus difficile. Nous le ferons au chapitre 8.

Solution: notez d'abord que lorsque $m > n$ il n'y a pas de fonctions biunivoque d'un ensemble avec m éléments à un ensemble avec n éléments.

Soit maintenant $m \leq n$. Supposons que les éléments du domaine soient un_1 , un_2 , ..., un_m . Il y a n façons pour choisir la valeur de la fonction à un_1 . Étant donné que la fonction est un à un, la valeur de la la fonction à un_2 peut être choisie de n à 1 façons (car la valeur utilisée pour un_1 ne peut pas être réutilisée). En général, la valeur de la fonction à a_k peut être choisie de $n - k + 1$ manières. Par la règle du produit, il y a $n (n - 1) (n - 2) \cdots (n - m + 1)$ fonctions biunivoque d'un ensemble avec m éléments à un avec n éléments.

Par exemple, il y a $5 \cdot 4 \cdot 3 = 60$ fonctions biunivoque d'un ensemble de trois éléments à un ensemble à cinq éléments. ▲

Exemple 8 **Le plan de numérotation téléphonique** Le *plan de numérotation nord - américain (PNNA)* précise la format des numéros de téléphone aux États-Unis, au Canada et dans de nombreuses autres parties de l'Amérique du Nord.UNE numéro de téléphone dans ce plan se compose de 10 chiffres, qui sont divisés en un indicatif régional à trois chiffres, un un code de bureau à trois chiffres et un code de station à quatre chiffres.Pour des raisons de signalisation, il sont certaines restrictions sur certains de ces chiffres. Pour spécifier le format autorisé, laissez - X représentent chacun un chiffre qui peut prendre l'une des valeurs 0 à 9, soit N désigne un chiffre qui peut prendre l'une des valeurs suivantes: les valeurs 2 à 9, et que Y désigne un chiffre qui doit être un 0 ou un 1. Deux plans de numérotation, qui sera appelé l'ancien plan et le nouveau plan seront discutés.(L'ancien plan, utilisé dans dans les années 60, a été remplacé par le nouveau plan, mais la récente croissance rapide de la demande de les numéros des téléphones portables et des appareils rendront à terme ce nouveau plan obsolète.Dans cet exemple, les lettres utilisées pour représenter les chiffres suivent les conventions de l'*Amérique* du *Nord Plan de numérotation* .) Comme nous le verrons, le nouveau plan permet d'utiliser plus de numéros.

Les projections actuelles sont qu'en 2038, il sera nécessaire d'ajouter un ou plus de chiffres vers le nord Téléphone américain Nombres.

Dans l'ancien plan, les formats de l'indicatif régional, de l'indicatif de bureau et du code de station sont NYX , NNX et $XXXX$, respectivement, de sorte que les numéros de téléphone aient la forme NYX - NNX - $XXXX$. Dans le nouveau plan, les formats de ces codes sont respectivement NXX , NXX et $XXXX$, de sorte que les numéros de téléphone ont la forme NXX - NXX - $XXXX$. Combien de numéros de téléphone nord-américains différents possible sous l'ancien plan et sous le nouveau plan?

Solution: selon la règle du produit, il existe $8 \cdot 2 \cdot 10 = 160$ indicatifs régionaux au format NYX et $8 \cdot 10 \cdot 10 = 800$ indicatifs régionaux au format NXX . De même, selon la règle du produit, il existe $8 \cdot 8 \cdot 10 = 640$ codes de bureau au format NNX . La règle du produit montre également qu'il existe $10 \cdot 10 \cdot 10 \cdot 10 = 10, 000$ codes de la station au format $XXXX$.

Notez que nous avons ignoré restrictions qui excluent Codes de station N11 pour la plupart des indicatifs régionaux.

Par conséquent, en appliquant à nouveau la règle du produit, il s'ensuit que l'ancien plan prévoit

$$160 \cdot 640 \cdot 10,000 = 1,024,000,000$$

différents numéros disponibles en Amérique du Nord. Dans le cadre du nouveau plan, il existe

$$800 \cdot 800 \cdot 10,000 = 6,400,000,000$$

différents numéros disponibles. ▲

EXEMPLE 9 Quelle est la valeur de k après le code suivant, où $n_1, n_2, \ldots, n_m$ sont des entiers positifs, a été exécuté?

```
k := 0
pour i1 := 1 à n1
   pour i2 := 1 à n2
          .
          .
          .
      pour im := 1 à nm
          k := k + 1
```

Solution: la valeur initiale de k est zéro. Chaque fois que la boucle imbriquée est parcourue, 1 est ajouté à k. Soit T_i la tâche de parcourir la i ème boucle. Ensuite, le nombre de fois que la boucle est parcourue est le nombre de façons d'effectuer les tâches $T_1, T_2, \ldots, T_m$. Le nombre de façons de réaliser la tâche T_j, $j = 1, 2, \ldots, m$, est n_j, car la j ème boucle est parcourue une fois pour chaque entier i_j avec $1 \le i_j \le n_j$. Par la règle du produit, il s'ensuit que la boucle imbriquée est parcourue $n_1 n_2 \cdots n_m$ fois. Par conséquent, la valeur finale de k est $n_1 n_2 \cdots n_m$. ▲

EXEMPLE 10 **Comptage de sous-ensembles d'un ensemble fini** Utilisez la règle de produit pour montrer que le nombre de différents sous-ensembles d'un ensemble fini S est $2^{|S|}$

Solution: Soit S un ensemble fini. Liste les éléments de S dans un ordre arbitraire. Rappel de Section 2.2 qu'il existe une correspondance biunivoque entre les sous-ensembles de S et les chaînes de bits de longueur $|S|$. A savoir, un sous-ensemble de S est associé à la chaîne de bits avec un 1 en i ème position si le i ème élément de la liste est dans le sous-ensemble, et un 0 dans cette position sinon. Par la règle du produit, il ya deux $2^{|S|}$ chaînes de bits de longueur $|S|$. Par conséquent, $|P(S)| = 2^{|S|}$. (Rappelons que nous avons utilisé des mathématiques induction pour prouver ce fait dans l'exemple 10 de la section 5.1.) ▲

La règle du produit est souvent formulée en termes d'ensembles de cette façon: si $A_1, A_2, \ldots, A_m$ sont finis ensembles, le nombre d'éléments dans le produit cartésien de ces ensembles est le produit de la nombre d'éléments dans chaque ensemble. Pour relier cela à la règle du produit, notez que la tâche de choisir un élément dans le produit cartésien $A_1 \times A_2 \times \cdots \times A_m$ se fait en choisissant un élément dans A_1, un élément dans A_2, ..., et un élément dans A_m. Par la règle du produit, il s'ensuit que

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|.$$

EXEMPLE 11 **ADN et génomes** Les informations héréditaires d'un organisme vivant sont codées en utilisant l'acide oxyribonucléique (ADN) ou, dans certains virus, l'acide ribonucléique (ARN). L'ADN et l'ARN sont molécules extrêmement complexes, avec différentes molécules interagissant dans une grande variété de façons de

permettre le processus vivant. Pour nos besoins, nous ne donnons que la description la plus brève de la façon dont l'ADN et l'ARN code les informations génétiques.

Les molécules d'ADN sont constituées de deux brins constitués de blocs appelés nucléotides. Chaque le nucléotide contient des sous-composants appelés **bases**, dont chacun est l'adénine (A), la cytosine (C), guanine (G) ou thymine (T). Les deux brins d'ADN sont maintenus ensemble par des liaisons hydrogène reliant différentes bases, avec une liaison A uniquement avec T et une liaison C uniquement avec G. L'ADN, l'ARN est simple brin, l'uracile (U) remplaçant la thymine comme base. Donc, dans l'ADN, le les paires de bases possibles sont AT et CG, tandis que dans l'ARN, elles sont AU et CG. L'ADN d'un vivant créature se compose de plusieurs morceaux d'ADN formant des chromosomes séparés. Un **gène** est un segment d'une molécule d'ADN qui code pour une protéine particulière. L'ensemble des informations génétiques d'un l'organisme est appelé son **génome**.

Les séquences de bases dans l'ADN et l'ARN codent pour de longues chaînes de protéines appelées acides aminés. Il existe 22 acides aminés essentiels pour l'homme. Nous pouvons rapidement voir qu'une séquence d'au au moins trois bases sont nécessaires pour coder ces 22 acides aminés différents. Première note, parce que il y a quatre possibilités pour chaque base dans l'ADN, A, C, G et T, selon la règle du produit, il y a $4^2 = 16 < 22$ séquences différentes de deux bases. Cependant, il existe $4^3 = 64$ séquences différentes de trois bases, qui fournissent suffisamment de séquences différentes pour coder les 22 acides aminés différents (même en tenant compte du fait que plusieurs séquences différentes de trois bases codent pour la même acide aminé).

L'ADN de simples créatures vivantes telles que les algues et les bactéries a entre 10^5 et 10^7 liens, où chaque lien est l'une des quatre bases possibles. Des organismes plus complexes, tels que les sectes, les oiseaux et les mammifères ont entre 10^8 et 10^{10} liens dans leur ADN. Donc, par le produit règle, il y a au moins 4^{10^5} différentes séquences de bases dans l'ADN d'organismes simples et au au moins 4^{10^8} différentes séquences de bases dans l'ADN d'organismes plus complexes. Ce sont à la fois des chiffres incroyablement énormes, ce qui explique pourquoi il existe une si grande variabilité entre les les organismes vivants. Au cours des dernières décennies, des techniques ont été développées pour déterminer le génome de différents organismes. La première étape consiste à localiser chaque gène dans l'ADN d'un organisme. La tâche suivante, appelée **séquençage des gènes**, est la détermination de la séquence de liens sur chaque gène. (Bien sûr, la séquence spécifique de plis sur ces gènes dépend de la partici- particulier représentatif d'une espèce dont l'ADN est analysé.) Par exemple, l'être humain le génome comprend environ 23 000 gènes, chacun avec 1 000 liens ou plus. Séquençage génétique les techniques tirent parti de nombreux algorithmes récemment développés et reposent sur de de nouvelles idées en combinatoire. De nombreux mathématiciens et informaticiens travaillent sur des problèmes impliquant des génomes, participant aux domaines en évolution rapide de la bioinformatique et du calcul la biologie. ▲

Bientôt ce ne sera plus ça coûteux d'avoir votre propre code génétique trouvé.

Nous introduisons maintenant la règle de somme.

LA RÈGLE DE SOMME Si une tâche peut être effectuée de l'une des n_1 façons ou de l'une des n_2 façons, où aucun de l'ensemble des n_1 voies n'est le même que n'importe lequel de l'ensemble des n_2 voies, alors il y a $n_1 + n_2$ façons d'accomplir la tâche.

L'exemple 12 illustre comment la règle de somme est utilisée.

EXEMPLE 12 Supposons qu'un membre de la faculté de mathématiques ou un étudiant qui est majeur en mathématiques est choisi comme représentant dans un comité universitaire. Combien de choix différents y a-t-il pour ce représentant s'il y a 37 membres de la faculté de mathématiques et 83 mathématiques majors et personne n'est à la fois membre du corps professoral et étudiant?

Solution: il y a 37 façons de choisir un membre de la faculté de mathématiques et 83 façons de choisir un élève qui est majeur en mathématiques. Choisir un membre des mathématiques la faculté n'est jamais la même chose que de choisir un étudiant qui est majeur en mathématiques parce que personne n'est

à la fois un membre du corps professoral et un étudiant. Par la règle de somme, il s'ensuit qu'il y a $37 + 83 = 120$ façons possibles de choisir ce représentant. ▲

Nous pouvons étendre la règle de somme à plus de deux tâches. Supposons qu'une tâche puisse être effectuée en un seul de n_1 voies, dans l'une des n_2 voies, ... , ou dans l'une des n_m façons, où aucun des n_i chemins de l'exécution de la tâche est la même que n'importe laquelle des n_j voies, pour toutes les paires i et j avec $1 \leq i < j \leq m$. Ensuite, le nombre de façons d'effectuer la tâche est $n_1 + n_2 + \cdots + n_m$. Cette version étendue du la règle de somme est souvent utile pour compter les problèmes, comme le montrent les exemples 13 et 14. Cette version du la règle de somme peut être prouvée en utilisant l'induction mathématique de la règle de somme pour deux ensembles (C'est Exercice 71.)

EXEMPLE 13 Un étudiant peut choisir un projet informatique dans l'une des trois listes. Les trois listes contiennent 23, 15, et 19 projets possibles, respectivement. Aucun projet ne figure sur plusieurs listes. Combien possible quels projets pouvez-vous choisir?

Solution: l'étudiant peut choisir un projet en sélectionnant un projet dans la première liste, la seconde ou la troisième liste. Puisqu'aucun projet n'est sur plus d'une liste, selon la règle de somme il y a $23 + 15 + 19 = 57$ façons de choisir un projet. ▲

EXEMPLE 14 Quelle est la valeur de k après le code suivant, où $n_1, n_2, \ldots, n_m$ sont des entiers positifs, a été exécuté?

$k := 0$

pour $i_1 := 1$ **à** n_1
    $k := k + 1$

pour $i_2 := 1$ **à** n_2
    $k := k + 1$

.
.
.
pour $i_m := 1$ **à** n_m
$k := k + 1$

Solution: la valeur initiale de k est zéro. Ce bloc de code est composé de m boucles différentes. Chaque fois qu'une boucle est parcourue, 1 est ajouté à k . Pour déterminer la valeur de k après que ce code a été exécuté, nous devons déterminer combien de fois nous traversons une boucle. Notez qu'il existe n_i façons de parcourir la i ème boucle. Parce que nous traversons une seule boucle à la fois, la règle de somme montre que la valeur finale de k , qui est le nombre de façons de parcourir l'une des m boucles est $n_1 + n_2 + \cdots + n_m$. ▲

La règle de somme peut être formulée en termes d'ensembles: Si $A_1, A_2, ..., A_m$ sont disjoints deux à deux ensembles finis, alors le nombre d'éléments dans l'union de ces ensembles est la somme des nombres de éléments dans les ensembles. Pour relier cela à notre énoncé de la règle de somme, notez qu'il existe $|A_i|$ façons de choisir un élément de A_i pour $i = 1, 2, ..., m$. Parce que les ensembles sont disjoints par paire, lorsque nous sélectionnons un élément dans l'un des ensembles A_i , nous ne sélectionnons pas également un élément dans un autre définir A_j . Par conséquent, selon la règle de somme, parce que nous ne pouvons pas sélectionner un élément parmi deux de ces ensembles en même temps, le nombre de façons de choisir un élément dans l'un des ensembles, qui est le nombre d'éléments dans l'union, est

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m| \text{ lorsque } A_i \cap A_j = \text{ pour tout } i, j.$$

Cette égalité ne s'applique que lorsque les ensembles en question sont disjoints deux à deux. La situation est bien plus compliqué lorsque ces ensembles ont des éléments en commun. Cette situation sera brièvement discuté plus loin dans cette section et discuté plus en détail au chapitre 8.

Problèmes de comptage plus complexes

De nombreux problèmes de comptage ne peuvent pas être résolus en utilisant uniquement la règle de somme ou uniquement la règle de produit. Cependant, de nombreux problèmes de comptage compliqués peuvent être résolus en utilisant ces deux règles dans combinaison. On commence par compter le nombre de noms de variables dans le langage de programmation DE BASE. (Dans les exercices, nous considérons le nombre de noms de variables dans JAVA.) Ensuite, nous allons compter le nombre de mots de passe valides soumis à un ensemble particulier de restrictions.

EXEMPLE 15 Dans une version du langage informatique BASIC, le nom d'une variable est une chaîne d'un ou deux caractères alphanumériques, où les majuscules et les minuscules ne sont pas distinguées.(Un *Le* caractère *alphanumérique* est soit l'une des 26 lettres anglaises, soit l'un des 10 chiffres.) De plus, un nom de variable doit commencer par une lettre et doit être différent des cinq chaînes de deux caractères réservés à la programmation. Combien de noms de variables différents existe-t-il dans cette version de BASIC?

Solution: Soit V égal au nombre de noms de variables différents dans cette version de BASIC. Soit V_1 être le nombre de ceux qui sont d'un caractère et V_2 le nombre de ceux qui sont deux Longs caractères. Ensuite, selon la règle de somme, $V = V_1 + V_2$. Notez que $V_1 = 26$, car un caractère le nom de la variable doit être une lettre. De plus, selon la règle du produit, il y a $26 \cdot 36$ chaînes de longueur deux commençant par une lettre et se terminant par un caractère alphanumérique. Cependant, cinq de ces sont exclus, donc $V_2 = 26 \cdot 36 - 5 = 931$. Par conséquent, il y a $V = V_1 + V_2 = 26 + 931 = 957$ noms différents pour les variables dans cette version de BASIC. ▲

EXEMPLE 16 Chaque utilisateur d'un système informatique a un mot de passe de six à huit caractères, où chaque caractère est une lettre majuscule ou un chiffre. Chaque mot de passe doit contenir au moins un chiffre. Combien de mots de passe possibles existe-t-il?

Solution: Soit P le nombre total de mots de passe possibles et P_6 , P_7 et P_8 désignent le nombre de mots de passe possibles de longueur 6, 7 et 8, respectivement. Par la règle de somme, $P = P_6 + P_7 + P_8$. Nous allons maintenant trouver P_6 , P_7 et P_8 . Trouver P_6 directement est difficile. Pour trouver P_6 c'est trouver plus facilement le nombre de chaînes de lettres majuscules et de chiffres de six caractères, y compris celles sans chiffres, et soustrayez-en le nombre de chaînes sans chiffres. Par la règle du produit, le nombre de chaînes de six caractères est 36^6 et le nombre de chaînes avec aucun chiffre n'est 26^6 . Par conséquent,

$$P_6 = 36^6 - 26^6 = 2,176,782,336 - 308,915,776 = 1,867,866,560.$$

De même, nous avons

$$P_7 = 36^7 - 26^7 = 78,364,164,096 - 8,031,810,176 = 70,332,353,920$$

et

$$P_8 = 36^8 - 26^8 = 2,821,109,907,456 - 208,827,064,576$$
$$= 2,612,282,842,880.$$

Par conséquent,

$$P = P_6 + P_7 + P_8 = 2,684,483,063,360.$$

▲

EXEMPLE 17 **Comptage des adresses Internet** Dans Internet, qui est constitué de ressources physiques interconnectées réseaux d'ordinateurs, chaque ordinateur (ou plus précisément, chaque connexion réseau d'un ordinateur) se voit attribuer une *adresse Internet* . Dans la version 4 du protocole Internet (IPv4), désormais utilisé,

Numéro de bit	0	1	2	3	4	8	16	24	31
Classe A	0			netid			hostid		
Classe B	1	0				netid		hostid	
Classe C	1	1	0			netid			hostid
Classe D	1	1	1	0			Adresse de multidiffusion		
Classe E	1	1	1	1	0		Adresse		

FIGURE 1 **Adresses Internet (IPv4).**

une adresse est une chaîne de 32 bits. Il commence par un *numéro de réseau* (*netid*). Le netid est suivi par un *numéro d'hôte* (*hostid*), qui identifie un ordinateur comme membre d'un réseau particulier.

Trois formes d'adresses sont utilisées, avec différents nombres de bits utilisés pour les netids et les hostids. **Les adresses de classe A** , utilisées pour les plus grands réseaux, sont composées de 0, suivi d'un netid 7 bits et d'un Hostid 24 bits. **Les adresses de classe B** , utilisées pour les réseaux de taille moyenne, se composent de 10, suivies de un netid 14 bits et un hostid 16 bits. **Les adresses de classe C** , utilisées pour les plus petits réseaux, se composent de 110, suivi d'un netid 21 bits et d'un hostid 8 bits. Il existe plusieurs restrictions sur les adresses en raison d'utilisations spéciales: 1111111 n'est pas disponible en tant que netid d'un réseau de classe A et les hostids composés de tous les 0 et de tous les 1 ne sont pas disponibles pour une utilisation dans aucun réseau. Un ordinateur sur Internet possède une adresse de classe A, de classe B ou de classe C. (Outre les classes A, B, et C, il existe également des adresses de classe D, réservées à une utilisation en multidiffusion plusieurs ordinateurs sont adressés en une seule fois, composé de 1110 suivis de 28 bits, et Adresses de classe E, réservées à un usage futur, composées de 11110 suivies de 27 bits. Ni Les adresses de classe D ou de classe E sont attribuées en tant qu'adresse IPv4 d'un ordinateur sur Internet.) La figure 1 illustre l'adressage IPv4. (Limitations du nombre de netids de classe A et de classe B ont rendu l'adressage IPv4 inadéquat; IPv6, une nouvelle version d'IP, utilise des adresses 128 bits pour résoudre ce problème.)

Le manque de disponibilité L'adresse IPv4 a devenir une crise!

Combien d'adresses IPv4 différentes sont disponibles pour les ordinateurs sur Internet?

Solution: Soit x le nombre d'adresses disponibles pour les ordinateurs sur Internet, et soit x_A, x_B et x_C indiquent respectivement le nombre d'adresses de classe A, de classe B et de classe C disponibles.

Par la règle de somme, $x = x_A + x_B + x_C$.

Pour trouver x_A, notez qu'il y a $2^7 - 1 = 127$ netids de classe A, rappelant que le netid 1111111 n'est pas disponible. Pour chaque netid, il y a $2^{24} - 2 = 16,777,214$ hostides, rappelant que le les hostides composés de tous les 0 et de tous les 1 ne sont pas disponibles. Par conséquent, $x_A = 127 \cdot 16,777,214 = 2,130,706,178$.

Pour trouver x_B et x_C, notez qu'il y a $2^{14} = 16,384$ netidés de classe B et $2^{21} = 2,097,152$ Netids de classe C. Pour chaque netid de classe B, il y a $2^{16} - 2 = 65,534$ hostides, et pour chaque Netid de classe C, il y a $2^8 - 2 = 254$ hostids, rappelant que dans chaque réseau les hostids composé de tous les 0 et tous les 1 ne sont pas disponibles. Par conséquent, $x_B = 1,073,709,056$ et $x_C = 532,676,608$.

Nous concluons que le nombre total d'adresses IPv4 disponibles est $x = x_A + x_B + x_C = 2,130,706,178 + 1,073,709,056 + 532,676,608 = 3,737,091,842$. ▲

La règle de soustraction (inclusion-exclusion pour deux ensembles)

Supposons qu'une tâche peut être effectuée de deux manières, mais que certaines des façons de le faire sont courantes dans les deux sens. Dans cette situation, nous ne pouvons pas utiliser la règle de somme pour compter le nombre de façons de faire la tâche. Si nous ajoutons le nombre de façons de faire les tâches de ces deux façons, nous obtenons un décompte du nombre total de façons de le faire, parce que les façons de faire la tâche qui sont communes aux deux les voies sont comptées deux fois. Pour compter correctement le nombre de façons d'effectuer les deux tâches, nous devons soustrayez le nombre de façons qui sont comptées deux fois. Cela nous amène à une règle de comptage importante.

Le comptage excessif est peut-être le plus courant erreur d'énumération.

LA RÈGLE DE SOUSTRACTION Si une tâche peut être effectuée de n_1 façons ou n_2 façons, alors la nombre de façons de faire la tâche est $n_1 + n_2$ moins le nombre de façons de faire la tâche qui sont commun aux deux façons différentes.

La règle de soustraction est également connue sous le nom de **principe d'inclusion-exclusion** , en particulier lorsque il est utilisé pour compter le nombre d'éléments dans l'union de deux ensembles. Supposons que A_1 et A_2 soient ensembles. Ensuite, il y a $|A_1|$ façons de sélectionner un élément parmi A_1 et $|A_2|$ façons de sélectionner un élément de A_2 . Le nombre de façons de sélectionner un élément de A_1 ou de A_2 , c'est-à-dire le nombre de façons de sélectionner un élément de leur union, est la somme du nombre de façons de sélectionner un élément de A_1 et le nombre de façons de sélectionner un élément de A_2 , moins le nombre de façons de sélectionnez un élément qui est à la fois dans A_1 et A_2 . Parce qu'il y a $|A_1 \cup A_2|$ façons de sélectionner un élément soit en A_1, soit en A_2 , et $|A_1 \cap A_2|$ façons de sélectionner un élément commun aux deux ensembles, nous avons

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Il s'agit de la formule donnée à la section 2.2 pour le nombre d'éléments dans l'union de deux ensembles.

L'exemple 18 illustre comment résoudre des problèmes de comptage en utilisant le principe de soustraction.

EXEMPLE 18 Combien de chaînes de bits de longueur huit commencent par un bit ou se terminent par les deux bits 00?

Solution: nous pouvons construire une chaîne de bits de longueur huit qui commence par un bit ou se termine avec les deux bits 00, en construisant une chaîne de bits de longueur huit commençant par 1 bit ou en la construction d'une chaîne de bits de longueur huit qui se termine par les deux bits 00. Nous pouvons construire un bit chaîne de longueur huit qui commence par un 1 sur $2^7 = 128$ voies. Cela suit la règle du produit, parce que le premier bit ne peut être choisi que dans un sens et chacun des sept autres bits peut être choisi de deux façons. De même, nous pouvons construire une chaîne de bits de longueur huit se terminant par les deux bits 00, en $2^6 = 64$ voies. Cela suit la règle du produit, car chacun des six premiers bits peut être choisi de deux manières et les deux derniers bits ne peuvent être choisis que d'une seule manière.

1

$2^7 = 128$ voies

0 0

$2^6 = 64$ voies

1 0 0

$2^5 = 32$ voies

Certaines des façons de construire une chaîne de bits de longueur huit commençant par un 1 sont les mêmes comme les moyens de construire une chaîne de bits de longueur huit qui se termine par les deux bits 00. Il y a $2^5 = 32$ façons de construire une telle chaîne. Cela suit la règle du produit, car le premier le bit ne peut être choisi que d'une seule manière, chacun des deuxième à sixième bits peut être choisi de deux manières, et les deux derniers bits peuvent être choisis d'une manière. Par conséquent, le nombre de chaînes de bits de longueur huit qui commencent par un 1 ou se terminent par un 00, ce qui équivaut au nombre de façons de construire une chaîne de bits de longueur huit qui commence par un 1 ou qui se termine par 00, est égal à $128 + 64 - 32 = 160$. ▲

Nous présentons un exemple qui illustre comment la formulation du principe d'inclusion - l'exclusion peut être utilisée pour résoudre des problèmes de comptage.

EXEMPLE 19 Une entreprise informatique reçoit 350 candidatures de diplômés en informatique pour un emploi ligne de nouveaux serveurs Web. Supposons que 220 de ces candidats se spécialisent en informatique, 147 avec une spécialisation en affaires et 51 avec une spécialisation en informatique et en affaires. Combien de ces candidats ne se sont spécialisés ni en informatique ni en affaires?

Solution: trouver le nombre de ces candidats qui ne se sont spécialisés ni en informatique ni en en affaires, on peut soustraire le nombre d'étudiants qui se sont spécialisés soit en informatique ou en affaires (ou les deux) du nombre total de candidats. Soit A_1 l'ensemble des étudiants qui spécialisé en informatique et A_2 l'ensemble des étudiants qui se sont spécialisés en affaires. Alors $A_1 \cup A_2$ est l'ensemble des étudiants qui se sont spécialisés en informatique ou en affaires (ou les deux), et $A_1 \cap A_2$ est le ensemble d'étudiants qui se sont spécialisés à la fois en informatique et en affaires.Par la règle de soustraction le nombre d'étudiants diplômés en informatique ou en affaires (ou les deux) est égal à

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316.$$

Nous concluons que 350 - 316 = 34 des candidats ne se sont qualifiés ni en informatique ni en affaires. ▲

La règle de soustraction, ou le principe d'inclusion-exclusion, peut être généralisé pour trouver le nombre de façons d'effectuer l'une des n tâches différentes ou, de manière équivalente, de trouver le nombre d'éléments dans l'union de n ensembles, chaque fois que n est un entier positif. Nous étudierons l'inclusion-exclusion et certaines de ses nombreuses applications au chapitre 8.

La règle de division

Nous avons introduit les règles de produit, de somme et de soustraction pour le comptage.Vous vous demandez peut-être s'il existe également une règle de division pour le comptage.En fait, il existe une telle règle, qui peut être utile pour résoudre certains types de problèmes d'énumération.

LA RÈGLE DE LA DIVISION Il existe n / d façons de faire une tâche si elle peut être effectuée en utilisant une procédure qui peut être effectuée de n façons, et pour chaque façon w , exactement d des n voies correspondent au chemin w .

Nous pouvons reformuler la règle de division en termes d'ensembles: « Si l'ensemble fini A est l'union de n pairwise sous-ensembles disjoints contenant chacun d éléments, alors $n = |A| / d$. "

On peut également formuler la règle de division en termes de fonctions: «Si f est une fonction de A à B où A et B sont des ensembles finis, et que pour chaque valeur $y \in B$ il y a exactement d valeurs $x \in A$ tel que $f(x) = y$ (auquel cas, on dit que f est d -to-one), alors $|B| = |A| / d$. "

Nous illustrons l'utilisation de la règle de division pour compter avec un exemple.

EXEMPLE 20 Combien de manières différentes existe-t-il pour asseoir quatre personnes autour d'une table circulaire, où deux les sièges sont considérés comme les mêmes lorsque chaque personne a le même voisin de gauche et le même bon voisin?

Solution: nous sélectionnons arbitrairement un siège à la table et l'étiquetons siège 1. Nous numérotons le reste du sièges dans l'ordre numérique, en procédant dans le sens horaire autour de la table.Notez qu'il existe quatre façons de sélectionner la personne pour le siège 1, trois façons de sélectionner la personne pour le siège 2, deux façons de sélectionner le personne pour le siège 3, et une façon de sélectionner la personne pour le siège 4. Ainsi, il y a 4!= 24 façons de commander les quatre personnes données pour ces sièges.Cependant, chacun des quatre choix pour le siège 1 mène au même arrangement, car nous distinguons deux arrangements seulement lorsque l'une des personnes a un autre voisin immédiat de gauche ou de droite immédiat.Parce qu'il y a quatre façons de choisir la personne du siège 1, par la règle de division ,il y a $24 / 4 = 6$ différents arrangements de sièges de quatre personnes autour de la table circulaire. ▲

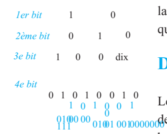


FIGURE 2 **Bit Chaînes de longueur Quatre sans 1s consécutifs.**

Diagrammes d'arbre

Les problèmes de comptage peuvent être résolus à l'aide de **diagrammes arborescents** . Un arbre se compose d'une racine, d'un nombre de branches quittant la racine et d'éventuelles branches supplémentaires quittant les extrémités d'autres branches. (Nous étudierons les arbres en détail au chapitre 11.) Pour utiliser les arbres dans le comptage, nous utilisons une branche pour représenter chaque choix possible. Nous représentons les résultats possibles par les feuilles, qui sont les extrémités des branches n'ayant pas d'autres branches commençant par elles.

Notez que lorsqu'un arbre est utilisé pour résoudre un problème de comptage, le nombre de choix dont la branche à suivre pour atteindre une feuille peut varier (voir l'exemple 21, par exemple).

Équipe gagnante montré en couleur

Équipe 2 Équipe 1

Jeu 1

Équipe 2 Équipe 1 Équipe 2 Équipe 1

Jeu 2

Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 2

Équipe 2 Équipe 1 *Game 3*

Équipe 1 Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 2

Équipe 2 Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 1 *Jeu 4*

Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 1 Équipe 2 Équipe 1 *Jeu 5*

FIGURE 3 **Trois meilleurs matchs sur cinq éliminatoires.**

EXEMPLE 21 Combien de chaînes de bits de longueur quatre n'ont pas deux 1 consécutifs?

Solution: L'arborescence de la figure 2 affiche toutes les chaînes de bits de longueur quatre sans deux secutive 1s. Nous voyons qu'il y a huit chaînes de bits de longueur quatre sans deux 1 consécutifs.▲

EXEMPLE 22 Une partie éliminatoire entre deux équipes comprend au plus cinq matchs. La première équipe qui remporte trois matchs remporte les éliminatoires. De combien de manières différentes les éliminatoires peuvent-elles se produire?

Solution: L'arborescence de la figure 3 affiche toutes les façons dont les séries éliminatoires peuvent se dérouler, gagnant de chaque match présenté. Nous voyons qu'il y a 20 façons différentes pour les séries éliminatoires de se produire. ▲

EXEMPLE 23 Supposons que les T-shirts «I Love New Jersey» existent en cinq tailles différentes: S, M, L, XL et XXL. Supposons en outre que chaque taille soit disponible en quatre couleurs, blanc, rouge, vert et noir, sauf pour XL, qui vient seulement en rouge, vert et noir, et XXL, qui vient seulement en vert et noir. Comment de nombreuses chemises différentes, une boutique de souvenirs doit-elle en avoir pour en avoir au moins une taille et couleur du T-shirt?

Solution: L'arborescence de la figure 4 affiche toutes les tailles et paires de couleurs possibles. Il s'ensuit que le propriétaire de la boutique de souvenirs doit stocker 17 T-shirts différents. ▲

W = blanc, R = rouge, G = vert, B = noir

S M L XL XXL

WRGB WRGB WRGBRGB GB

FIGURE 4 **Compter les variétés de T-shirts.**

Des exercices

1. Il existe 18 majeures en mathématiques et 325 scien-
majeures dans un collège.

a) De combien de façons peut-on choisir deux représentants de sorte que l'un est une majeure en mathématiques et l'autre est un majeure en informatique?

b) De combien de façons un représentant peut-il être choisi qui est soit une majeure en mathématiques ou une science informatique majeure?

2. Un immeuble de bureaux de 27 étages et 37 bureaux à chaque étage. Combien de bureaux y a-t-il dans le bâtiment?

3. Un test à choix multiple contient 10 questions. Il y a quatre réponses possibles pour chaque question.

a) De combien de façons un élève peut-il répondre aux questions au test si l'étudiant répond à toutes les questions?

b) De combien de façons un élève peut-il répondre aux questions sur le test si l'élève peut laisser des réponses vides?

4. Une marque particulière de chemise est disponible en 12 couleurs, a un homme version et une version féminine, et est disponible en trois tailles pour chaque sexe. Combien de types différents de cette chemise sont fait?

5. Six compagnies aériennes différentes volent de New York à Denver et sept volent de Denver à San Francisco. Combien de différentes paires de compagnies aériennes peuvent vous choisir un voyage de New York à San Francisco via Denver, quand vous choisissez une compagnie aérienne pour le vol vers Denver et une compagnie aérienne pour le vol de suite à San Francisco?

6. Il existe quatre itinéraires automobiles majeurs de Boston à Détroit et six de Détroit à Los Angeles. Combien de grands les routes automatiques sont là de Boston à Los Angeles via De-troit?

7. Combien d'initiales de trois lettres différentes les gens peuvent-ils avoir?

8. Combien d'initiales de trois lettres différentes sans aucun des les lettres peuvent-elles être répétées?

9. Combien d'initiales de trois lettres différentes existe-t-il gin avec un *A* ?

10. Combien y a-t-il de chaînes de bits de longueur huit?

11. Combien de chaînes de bits de longueur dix commencent et finissent avec un 1?

12. Combien de chaînes de bits y a-t-il de longueur six ou moins, pas compter la chaîne vide?

13. Combien de chaînes de bits dont la longueur ne dépasse pas n , où n est un entier positif, composé entièrement de 1, sans compter la chaîne vide?

14. Combien de chaînes de bits de longueur n , où n est positif entier, début et fin avec 1s?

15. Combien y a-t-il de chaînes de lettres minuscules quatre ou moins, sans compter la chaîne vide?

16. Combien de chaînes y a-t-il de quatre lettres minuscules qui avoir la lettre x en eux?

17. Combien de chaînes de cinq caractères ASCII contiennent le caractère @ (signe «at») au moins une fois? [*Remarque:* il y a 128 caractères ASCII différents.

18. Combien de séquences d'ADN à 5 éléments

a) se terminent par A?

b) commencer par T et finir par G?

c) ne contient que A et T?

d) ne contiennent pas de C?

19. Combien de séquences d'ARN à 6 éléments

a) ne contient pas U?

b) se terminent par GU?

c) commencer par C?

d) ne contient que A ou U?

20. Combien d'entiers positifs entre 5 et 31

a) sont divisibles par 3? Quels sont ces entiers?

b) sont divisibles par 4? Quels sont ces entiers?

c) sont divisibles par 3 et par 4? Quels sont ces entiers?

21. Combien d'entiers positifs entre 50 et 100

a) sont divisibles par 7? Quels entiers sont-ils?

b) sont divisibles par 11? Quels sont ces entiers?

c) sont divisibles à la fois par 7 et 11? Quels entiers sont celles-ci?

22. Combien d'entiers positifs moins de 1000

a) sont divisibles par 7?

b) sont divisibles par 7 mais pas par 11?

c) sont divisibles à la fois par 7 et 11?

d) sont divisibles par 7 ou 11?

e) sont divisibles par exactement l'un de 7 et 11?

f) ne sont divisibles ni par 7 ni par 11?

g) ont des chiffres distincts?

h) ont des chiffres distincts et sont pairs?

23. Combien d'entiers positifs compris entre 100 et 999 sive

a) sont divisibles par 7?

b) sont bizarres?

c) ont les mêmes trois chiffres décimaux?

d) ne sont pas divisibles par 4?

e) sont divisibles par 3 ou 4?

f) ne sont pas divisibles par 3 ou 4?

g) sont divisibles par 3 mais pas par 4?

h) sont divisibles par 3 et 4?

24. Combien d'entiers positifs entre 1 000 et 9 999 clusive

a) sont divisibles par 9?

b) sont pairs?

c) ont des chiffres distincts?

d) ne sont pas divisibles par 3?

e) sont divisibles par 5 ou 7?

f) ne sont pas divisibles par 5 ou 7?

g) sont divisibles par 5 mais pas par 7?

h) sont divisibles par 5 et 7?

Épisode 418

25. Combien de chaînes de trois chiffres décimaux

a) ne contiennent pas trois fois le même chiffre?

b) commence par un chiffre impair?

c) ont exactement deux chiffres qui sont 4s?

26. Combien de chaînes de quatre chiffres décimaux

a) ne contiennent pas deux fois le même chiffre?

b) se terminent par un chiffre pair?

c) a exactement trois chiffres qui sont 9s?

27. Un comité est composé d'un représentant de chacun des 50 États des États-Unis, où le représentant d'un État est le gouverneur ou un

35. Combien de fonctions un à un existe-t-il à partir d'un ensemble avec cinq éléments à des ensembles avec le nombre suivant d'élé-ments?

a) 4 **b)** 5 **c)** 6 **d)** 7

36. Combien de fonctions y a-t-il dans l'ensemble $\{1, 2, ..., n\}$, où n est un entier positif, à l'ensemble $\{0, 1\}$?

37. Combien de fonctions y a-t-il dans l'ensemble $\{1, 2, ..., n\}$, où n est un entier positif, à l'ensemble $\{0, 1\}$

a) qui sont un à un?

b) qui attribuent 0 à la fois à 1 et à n ?

c) qui attribuent 1 à exactement l'un des entiers positifs des deux sénateurs de cet état. Combien de façons là pour former ce comité?

28. Combien de plaques d'immatriculation peuvent être faites en utilisant trois chiffres suivis de trois lettres anglaises majuscules ou trois lettres anglaises majuscules suivies de trois chiffres?

29. Combien de plaques d'immatriculation peuvent être fabriquées à l'aide de deux lettres anglaises majuscules suivies de quatre ou deux chiffres chiffres suivis de quatre lettres anglaises majuscules?

30. Combien de plaques d'immatriculation peuvent être fabriquées en utilisant trois lettres anglaises majuscules suivies de trois ou quatre chiffres lettres anglaises majuscules suivies de deux chiffres?

31. Combien de plaques d'immatriculation peuvent être faites en utilisant deux ou trois lettres anglaises majuscules suivies de deux ou trois chiffres?

32. Combien de chaînes de huit lettres anglaises majuscules sont Là

a) si les lettres peuvent être répétées?
b) si aucune lettre ne peut être répétée?
c) qui commencent par X, si les lettres peuvent être répétées?
d) qui commencent par X, si aucune lettre ne peut être répétée?
e) qui commencent et se terminent par X, si les lettres peuvent être répétées?
f) commençant par les lettres BO (dans cet ordre), si les lettres peut être répété?
g) commençant et finissant par les lettres BO (dans cet ordre), si les lettres peuvent être répétées?
h) commençant ou finissant par les lettres BO (dans cet ordre), si les lettres peuvent être répétées?

33. Combien de chaînes de huit lettres anglaises y a-t-il

a) qui ne contiennent pas de voyelles, si les lettres peuvent être répétées?
b) qui ne contiennent pas de voyelles, si les lettres ne peuvent pas être répétées?
c) qui commencent par une voyelle, si les lettres peuvent être répétées?
d) qui commencent par une voyelle, si les lettres ne peuvent pas être répétées?
e) qui contiennent au moins une voyelle, si des lettres peuvent être tourbé?
f) qui contiennent exactement une voyelle, si des lettres peuvent être tourbé?
g) commençant par X et contenant au moins une voyelle, si les lettres peuvent être répétées?
h) commençant et finissant par X et contenant au moins un voyelle, si les lettres peuvent être répétées?

34. Combien de fonctions différentes existe-t-il dans un 10 éléments en ensembles avec les nombres d'éléments suivants ments?

a) 2 **b)** 3 **c)** 4 **d)** 5

moins de n ?

38. Combien y a-t-il de fonctions partielles (voir section 2.3) d'un ensemble avec cinq éléments à des ensembles avec chacun de ces nombre d'éléments?

a) 1 **b)** 2 **c)** 5 **d)** 9

39. Combien de fonctions partielles (voir la définition 13 de la section 2.3) existe-t-il d'un ensemble avec m éléments à un ensemble avec n éléments, où m et n sont des entiers positifs?

40. Combien de sous-ensembles d'un ensemble de 100 éléments ont plus qu'un élément?

41. Un **palindrome** est une chaîne dont l'inversion est identique à la chaîne. Combien de chaînes de bits de longueur n sont des palindromes?

42. Combien de séquences d'ADN à 4 éléments

a) ne contiennent pas la base T?
b) contenir la séquence ACG?
c) contiennent les quatre bases A, T, C et G?
d) contenir exactement trois des quatre bases A, T, C et G?

43. Combien de séquences d'ARN à 4 éléments

a) contenir la base U?
b) ne contiennent pas la séquence CUG?
c) ne contiennent pas les quatre bases A, U, C et G?
d) contenir exactement deux des quatre bases A, U, C et G?

44. Combien y a-t-il de façons de faire asseoir quatre personnes sur un groupe de dix autour d'une table circulaire où se trouvent deux sièges considéré de la même façon quand tout le monde a le même voisin de gauche et de droite immédiat?

45. Combien y a-t-il de façons d'asseoir six personnes autour d'un table spécifique où deux sièges sont considérés comme identiques quand tout le monde a les mêmes deux voisins sans se Gardez-vous s'ils sont voisins de droite ou de gauche?

46. De combien de façons un photographe lors d'un mariage peut-il gamme 6 personnes d'affilée d'un groupe de 10 personnes, où la mariée et le marié sont parmi ces 10 personnes, si

a) la mariée doit être sur la photo?
b) les mariés doivent être sur la photo?
c) exactement l'un des mariés est sur la photo ture?

47. De combien de façons un photographe lors d'un mariage peut-il gamme de six personnes d'affilée, y compris la mariée et le marié, si

a) la mariée doit être à côté du marié?
b) la mariée n'est pas à côté du marié?
c) la mariée est positionnée quelque part à gauche de la jeune marié?

Épisode 419

48. Combien de chaînes de bits de longueur sept commencent par deux 0 ou se terminent par trois 1?

49. Combien de chaînes de bits de longueur 10 commencent soit par trois 0 ou se termine par deux 0?

∗ **50.** Combien de chaînes de bits de longueur 10 contiennent soit cinq con- 0 ou cinq 1 consécutifs?

∗∗ **51.** Combien de chaînes de bits de longueur huit contiennent trois 0 consécutifs ou quatre 1 consécutifs?

52. Chaque élève d'une classe de mathématiques discrète est soit un informatique ou une majeure en mathématiques ou est un joint majeur dans ces deux matières. Combien d'étudiants sont classe s'il y a 38 majors en informatique (y compris avec des majeures conjointes), 23 majeures en mathématiques (y majeures), et 7 majeures conjointes?

53. Combien d'entiers positifs ne dépassant pas 100 sont divisés ible par 4 ou par 6?

54. Combien d'initiales différentes peut-on avoir si une personne a au moins deux, mais pas plus de cinq, différentes initiales? Supposons que chaque initiale est l'une des 26 lettres majuscules de la langue anglaise.

55. Supposons qu'un mot de passe pour un système informatique doit avoir au moins 8, mais pas plus de 12, où chacun le mot de passe est une lettre anglaise minuscule, une lettre majuscule en anglais, un chiffre ou l'un des six caractères

59. Supposons qu'à un moment futur, chaque téléphone du le monde se voit attribuer un numéro contenant un code de pays 1 à 3 chiffres, c'est-à-dire de la forme X , XX ou XXX , suivi d'un numéro de téléphone à 10 chiffres du formulaire NXX - NXX - $XXXX$ (comme décrit dans l'exemple 8). Comment de nombreux numéros de téléphone différents seraient disponibles dans le monde sous ce plan de numérotation?

60. Une clé du cryptosystème Vigenère est une chaîne d'anglais lettres, où le cas des lettres n'a pas d'importance. Comment de nombreuses clés différentes pour ce cryptosystème sont là avec trois, quatre, cinq ou six lettres?

61. Une clé de confidentialité équivalente filaire (WEP) pour un réseau délité (WiFi) est une chaîne de 10, 26 ou 58 chiffres hexadécimaux. Combien de clés WEP différentes sont Là?

62. Supposons que p et q sont des nombres premiers et que $n = pq$. Utilisez le principe de l'inclusion-exclusion pour trouver le nombre nombre d'entiers positifs ne dépassant pas n qui sont relativement premier à n .

63. Utilisez le principe de l'inclusion-exclusion pour trouver le nombre d'entiers positifs inférieurs à 1 000 000 qui ne sont pas divisible par 4 ou par 6.

64. Utilisez un arbre pour trouver le nombre de chaînes de bits de longueur quatre sans trois 0 consécutifs.

65. Combien y a-t-il de façons d'organiser les lettres a , b , c , et d tel que a ne soit pas immédiatement suivi de b ?

caractères spéciaux $*$, $>$, $<$, !, + et =.

a) Combien de mots de passe différents sont disponibles pour cela Système d'ordinateur?

b) Combien de ces mots de passe contiennent au moins un apparition d'au moins un des six caractères spéciaux?

c) À l'aide de votre réponse à la partie (a), déterminez combien de temps prend un pirate pour essayer tous les mots de passe possibles, en supposant que cela prend une nanoseconde à un pirate pour vérifier chaque mot de passe possible.

56. Le nom d'une variable dans le langage de programmation C est une chaîne qui peut contenir des lettres majuscules, des minuscules caractères, chiffres ou traits de soulignement. De plus, le premier caractère de la chaîne doit être une lettre, en majuscule ou en minuscule, ou un trait de soulignement. Si le nom d'une variable est déterminé par ses huit premiers caractères, combien de variables différentes peut être nommé en C? (Notez que le nom d'une variable peut contenir moins de huit caractères.)

57. Le nom d'une variable dans la langue de programmation JAVA la jauge est une chaîne de 1 à 65 535 caractères, inclus, où chaque caractère peut être une majuscule ou un une lettre minuscule, un signe dollar, un trait de soulignement ou un chiffre, sauf que le premier caractère ne doit pas être un chiffre. Dissuader-exploiter le nombre de noms de variables différents dans JAVA.

58. Union internationale des télécommunications (UIT) précise qu'un numéro de téléphone doit être composé d'un essayez le code avec entre 1 et 3 chiffres, sauf que le code 0 n'est pas disponible pour être utilisé comme code de pays, suivi de un nombre d'au plus 15 chiffres. Combien disponibles les numéros de téléphone possibles sont là qui répondent à ces restrictions?

66. Utilisez un diagramme arborescent pour trouver le nombre de World Series peut se produire, où la première équipe qui gagne quatre matchs sur sept remportent la série.

67. Utilisez un arbre pour déterminer le nombre de sous-ensembles de {3 , 7 , 9 , 11 , 24} avec la propriété que la somme des éléments du sous-ensemble est inférieur à 28.

68. a) Supposons qu'un magasin vend six variétés de boissons gazeuses: cola, soda au gingembre, orange, racinette, limonade et soda à la crème. Utilisez un arbre pour déterminer le nombre de différents types de bouteilles que le magasin doit avoir toutes les variétés disponibles dans des bouteilles de toutes tailles si sont disponibles en bouteilles de 12 onces, tout sauf ade sont disponibles en bouteilles de 20 onces, seulement cola et le gingembre est disponible en bouteilles de 32 onces, et tout sauf limonade et crème soda sont disponibles en 64 onces bouteilles?

b) Répondez à la question dans la partie (a) en utilisant des règles de comptage.

69. a) Supposons qu'un style populaire de chaussure de course soit aussi bien pour les hommes que pour les femmes. La chaussure de la femme est disponible en tailles 6, 7, 8 et 9, et la chaussure pour homme existe en tailles 8, 9, 10, 11 et 12. La chaussure homme vient en blanc et noir, tandis que la chaussure de la femme vient en blanc, rouge et noir. Utilisez un arbre pour déterminer le nombre de chaussures différentes qu'un magasin doit stocker pour avoir au moins une paire de ce type de chaussure de course pour toutes les tailles et couleurs disponibles pour les deux hommes et femmes.

b) Répondez à la question dans la partie (a) en utilisant des règles de comptage.

$*$ **70.** Utilisez la règle du produit pour montrer qu'il y a 2^{2^n} différent tables de vérité pour les propositions dans *n* variables.

71. Utiliser l'induction mathématique pour prouver la règle de somme pour *m* tâches de la règle de somme pour deux tâches.

72. Utiliser l'induction mathématique pour prouver la règle du produit pour *m* tâches à partir de la règle de produit pour deux tâches.

73. Combien de diagonales un polygone convexe avec *n* côtés avoir? (Rappelons qu'un polygone est convexe si chaque ligne se ment reliant deux points à l'intérieur ou à la limite de le polygone se situe entièrement dans cet ensemble et qu'une diag-nal d'un polygone est un segment de ligne reliant deux sommets qui ne sont pas adjacentes.)

74. Les données sont transmises sur Internet dans des **datagrammes** , qui sont des blocs de bits structurés. Chaque datagramme contient des informations d'en-tête organisées en un maximum de 14 domaines différents (spécifiant beaucoup de choses, y compris les adresses source et de destination) et une zone de données contient les données réelles qui sont transmises. Un de 14 champs d'en-tête est le **champ de longueur d'en-tête** (désigné par HLEN), qui est spécifié par le protocole comme étant 4 bits long et qui spécifie la longueur d'en-tête en termes de 32 bits blocs de bits. Par exemple, si HLEN = 0110, l'en-tête est composé de six blocs 32 bits. Un autre de l'en-tête 14 champs est le **champ de longueur totale de** 16 bits (indiqué par TOTAL LENGTH), qui spécifie la longueur en bits du datagramme entier, y compris les deux champs d'en-tête et la zone de données. La longueur de la zone de données est le total longueur du datagramme moins la longueur de l'en-tête.

a) La plus grande valeur possible de LONGUEUR TOTALE (qui est de 16 bits) détermine le maximum longueur totale en octets (blocs de 8 bits) d'un Internet datagramme. Quelle est cette valeur?

b) La plus grande valeur possible de HLEN (qui est de 4 bits long) détermine la longueur totale maximale de l'en-tête en blocs 32 bits. Quelle est cette valeur? Quel est le longueur totale maximale de l'en-tête en octets?

c) La longueur minimale (et la plus courante) de l'en-tête est 20 octets. Quelle est la longueur totale maximale en octets de la zone de données d'un datagramme Internet?

d) Combien de chaînes d'octets différentes dans la zone de données peut être transmis si la longueur de l'en-tête est de 20 octets et la longueur totale est aussi longue que possible?

Le principe du pigeonnier

introduction

Supposons qu'un troupeau de 20 pigeons vole dans un ensemble de 19 trous pour se percherParce qu'il y a 20 pigeons mais seulement 19 pigeonniers, au moins un de ces 19 pigeonniers doit avoir au moins deux des pigeons dedans. Pour voir pourquoi cela est vrai, notez que si chaque pigeonnier avait au plus un pigeon dedans, 19 pigeons au maximum, un par trou, pourraient être accueillis.Cela illustre un principe général appelé le **principe** du **pigeonnier** , qui stipule que s'il y a plus de pigeons que de pigeonniers, alors il doit y avoir au moins un pigeonnier avec au moins deux pigeons (voir figure 1).De Bien sûr, ce principe s'applique à d'autres objets que les pigeons et les pigeonniers.

THÉORÈME 1 **LE PRINCIPE PIGEONHOLE** Si k est un entier positif et $k + 1$ ou plusieurs objets sont placés dans k cases, puis il y a au moins une case contenant deux ou plusieurs des objets.

(une) b) (c)

FIGURE 1 Il y a plus de pigeons que de pigeonniers.

Preuve: Nous prouvons le principe du pigeonnier à l'aide d'une preuve par contraposition. Supposons qu'aucun des les k cases contiennent plus d'un objet. Le nombre total d'objets serait alors au plus k . C'est une contradiction, car il y a au moins $k + 1$ objets.

Le principe du pigeonnier est également appelé **principe du tiroir Dirichlet** , après le XIXe siècle mathématicien allemand G. Lejeune Dirichlet, qui a souvent utilisé ce principe dans son travail. (Dirichlet n'était pas la première personne à utiliser ce principe; une démonstration qu'il y avait au moins deux Parisiens avec le même nombre de cheveux sur la tête remontent au XVIIe siècle - voir l'exercice 33.) Il s'agit d'une technique de preuve supplémentaire importante qui complète celles que nous avons développé dans les chapitres précédents. Nous l'introduisons dans ce chapitre en raison de ses nombreux applications à la combinatoire.

Nous illustrerons l'utilité du principe du pigeonnier. Nous montrons d'abord qu'il peut être utilisé pour prouver un corollaire utile sur les fonctions.

COROLLARY 1 Une fonction f d'un ensemble avec $k + 1$ ou plusieurs éléments à un ensemble avec k éléments n'est pas biunivoque.

Preuve: Supposons que pour chaque élément y dans le codomaine de f, nous avons une boîte qui contient tous éléments x du domaine de f tels que $f(x) = y$. Parce que le domaine contient $k + 1$ ou plus éléments et le codomaine ne contient que k éléments, le principe du pigeonhole nous dit que l'on de ces cases contient deux ou plusieurs éléments x du domaine. Cela signifie que f ne peut pas être Un par un.

Les exemples 1 à 3 montrent comment le principe du pigeonnier est utilisé.

EXEMPLE 1 Parmi tout groupe de 367 personnes, il doit y en avoir au moins deux avec le même anniversaire, car il n'y a que 366 anniversaires possibles. ▲

EXEMPLE 2 Dans tout groupe de 27 mots anglais, il doit y en avoir au moins deux commençant par la même lettre, car il y a 26 lettres dans l'alphabet anglais. ▲

EXEMPLE 3 Combien d'étudiants doivent être dans une classe pour garantir qu'au moins deux étudiants reçoivent le même score à l'examen final, si l'examen est noté sur une échelle de 0 à 100 points?

Solution: Il y a 101 scores possibles sur la finale. Le principe du pigeonnier montre que parmi Pour 102 élèves, il doit y avoir au moins 2 élèves avec le même score. ▲

G. LEJEUNE DIRICHLET (1805–1859) G. Lejeune Dirichlet est né dans une famille belge vivant près de Cologne, Allemagne. Son père était maître de poste. Il est devenu passionné de mathématiques à un jeune âge. Il dépensait tout son argent de réserve pour des livres de mathématiques au moment où il est entré au lycée de Bonn 12 ans. À 14 ans, il entre au Collège des Jésuites de Cologne et à 16 ans il commence ses études à l'Université de Paris. En 1825, il est retourné en Allemagne et a été nommé à un poste à l'Université de Breslau. En 1828, il déménage à l'Université de Berlin. En 1855, il est choisi pour succéder à Gauss à l'Université de Göttingen. Dirichlet serait la première personne à maîtriser les *Disquisitiones Arithmeticae de* Gauss , apparus 20 ans plus tôt. Il en aurait gardé une copie à ses côtés, même en voyage. Dirichlet a fait de nombreuses découvertes importantes en théorie des nombres, y compris le théorème selon lequel il existe une infinité de nombres premiers dans les progressions arithmétiques $an + b$ lorsque a et b sont relativement prime. Il a prouvé le cas $n = 5$ du dernier théorème de Fermat, qu'il n'y a pas de solutions non triviales en nombres entiers à $x^5 + y^5 = z^5$. Dirichlet a également apporté de nombreuses contributions à l'analyse. Dirichlet était considéré comme un excellent enseignant qui pouvait expliquer des idées avec grande clarté. Il était marié à Rebecca Mendelssohn, l'une des sœurs du compositeur Frederick Mendelssohn.

Le principe du pigeonhole est un outil utile dans de nombreuses preuves, y compris les preuves de surprendre résultats, tels que ceux donnés dans l'exemple 4.

EXEMPLE 4 Montrer que pour chaque entier *n,* il existe un multiple de *n* qui n'a que 0 et 1 dans sa décimale expansion.

Solution: Soit *n* un entier positif. Considérons les $n + 1$ entiers 1 , 11 , 111 , ..., 11 ... 1 (où le dernier entier de cette liste est l'entier avec $n + 1$ 1s dans son expansion décimale). Notez qu'il sont *n* restes possibles lorsqu'un entier est divisé par *n* . Parce qu'il y a $n + 1$ entiers dans cette liste, selon le principe du pigeonhole, il doit y avoir deux avec le même reste lorsqu'ils sont divisés par *n* . Le plus grand de ces entiers moins le plus petit est un multiple de *n* , qui a une décimale expansion composée entièrement de 0 et de 1. ▲

Le principe du pigeonnier généralisé

Le principe du pigeonhole stipule qu'il doit y avoir au moins deux objets dans la même boîte lorsque il y a plus d'objets que de boîtes. Cependant, encore plus peut être dit lorsque le nombre d'objets dépasse un multiple du nombre de cases. Par exemple, parmi n'importe quel ensemble de 21 chiffres décimaux il doit y en avoir 3 identiques. Cela suit parce que lorsque 21 objets sont distribués dans 10 boîtes, une boîte doit avoir plus de 2 objets.

THÉORÈME 2 **LE PRINCIPE GÉNÉRALISÉ DES PIGEONS** Si *N* objets sont placés dans *k* boîtes, alors il y a au moins une boîte contenant au moins $\lceil N / k \rceil$ objets.

Preuve: Nous utiliserons une preuve par contraposition. Supposons qu'aucune des cases ne contienne plus que $\lceil N / k \rceil - 1$ objets. Ensuite, le nombre total d'objets est au maximum

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = N,$$

où l'inégalité $\lceil N / k \rceil < (N / k) + 1$ a été utilisée. Ceci est une contradiction car il sont un total de *N* objets.

Un type de problème courant demande le nombre minimum d'objets tel qu'au moins *r* de ces objets doivent se trouver dans l'une des *k* cases lorsque ces objets sont répartis entre les cases. Lorsque nous avons *N* objets, le principe du pigeonnier généralisé nous dit qu'il doit y avoir au moins *r* des objets dans l'une des cases tant que $\lceil N / k \rceil \geq r$. Le plus petit entier *N* avec $N / k > r - 1$, à savoir, $N = k(r - 1) + 1$, est le plus petit entier satisfaisant l'inégalité $\lceil N / k \rceil \geq r$. Pourrait une valeur plus petite de *N* suffit? La réponse est non, car si nous avions $k(r - 1)$ objets, nous pourrions mettez $r - 1$ d'entre eux dans chacune des *k* cases et aucune case n'aurait au moins *r* objets.

Lorsque vous pensez à des problèmes de ce type, il est utile de considérer comment vous pouvez éviter au moins *r* objets dans l'une des cases lorsque vous ajoutez des objets successifs. Pour éviter d'ajouter un *r* e objet à n'importe quelle boîte, vous vous retrouvez finalement avec $r - 1$ objets dans chaque boîte. Il n'y a aucun moyen d'ajouter le objet suivant sans mettre un *r* e objet dans cette case.

Les exemples 5 à 8 illustrent l'application du principe généralisé des trous de pigeonnier.

EXEMPLE 5 Sur 100 personnes, il y a au moins $\lceil 100 / 12 \rceil = 9$ qui sont nés le même mois. ▲

EXEMPLE 6 Quel est le nombre minimum d'élèves requis dans une classe de mathématiques discrète pour être sûr qu'au moins six recevront le même grade, s'il y a cinq grades possibles, A, B, C, D et F?

Solution: le nombre minimum d'étudiants requis pour garantir qu'au moins six étudiants reçoivent la même note est le plus petit entier N tel que $\lceil N / 5 \rceil = 6$. Le plus petit entier est $N = 5 \cdot 5 + 1 = 26$. Si vous n'avez que 25 étudiants, il est possible qu'il y en ait cinq qui ont reçu chaque année de sorte qu'aucun élève n'ait reçu la même année. Ainsi, 26 est le minimum nombre d'élèves nécessaires pour garantir qu'au moins six élèves recevront la même note. ▲

EXEMPLE 7 **a)** Combien de cartes doivent être sélectionnées dans un jeu standard de 52 cartes pour garantir qu'au moins trois cartes de la même couleur sont choisies?
b) Combien faut-il sélectionner pour garantir qu'au moins trois cœurs sont sélectionnés?

Un deck standard de 52 cartes a 13 types de cartes, avec quatre cartes de chacun de type, un dans chaque des quatre costumes, coeurs, diamants, bêches et clubs.

Solution: **a)** Supposons qu'il y ait quatre cases, une pour chaque couleur, et que les cartes sont sélectionnées, elles sont placé dans la boîte réservée aux cartes de cette couleur. En utilisant le principe du pigeonnier généralisé, on voit que si N cartes sont sélectionnées, il y a au moins une case contenant au moins $\lceil N / 4 \rceil$ cartes. Par conséquent, nous savons qu'au moins trois cartes d'une même couleur sont sélectionnées si $\lceil N / 4 \rceil \geq 3$. Le le plus petit entier N tel que $\lceil N / 4 \rceil \geq 3$ soit $N = 2 \cdot 4 + 1 = 9$, donc neuf cartes suffisent. Notez que si huit cartes sont sélectionnées, il est possible d'avoir deux cartes de chaque couleur, donc plus de huit cartes sont nécessaires. Par conséquent, neuf cartes doivent être sélectionnées pour garantir qu'au moins trois cartes de un costume est choisi. Une bonne façon d'y penser est de noter qu'après la huitième carte choisi, il n'y a aucun moyen d'éviter d'avoir une troisième carte d'une couleur.

b) Nous n'utilisons pas le principe généralisé des pigeonniers pour répondre à cette question, car nous voulons pour vous assurer qu'il y a trois coeurs, pas seulement trois cartes d'une même couleur. Notez que dans le pire cas, nous pouvons sélectionner tous les clubs, diamants et piques, 39 cartes en tout, avant de sélectionner un seul cœur. Les trois prochaines cartes seront toutes de cœur, il nous faudra donc peut-être sélectionner 42 cartes pour en obtenir trois. cœurs. ▲

EXEMPLE 8 Quel est le moins d'indicatifs régionaux nécessaires pour garantir que les 25 millions de téléphones dans un état peut-on attribuer des numéros de téléphone distincts à 10 chiffres?(Supposons que les numéros de téléphone sont le formulaire NXX - NXX - $XXXX$, où les trois premiers chiffres forment l'indicatif régional, N représente un chiffre de 2 à 9 inclus, et X représente n'importe quel chiffre.)

Solution: il existe huit millions de numéros de téléphone différents sous la forme NXX - $XXXX$ (comme indiqué dans l'exemple 8 de la section 6.1). Par conséquent, selon le principe du pigeonnier généralisé, parmi 25 millions téléphones, au moins $\lceil 25,000,000 / 8,000,000 \rceil = 4$ d'entre eux doivent avoir des numéros de téléphone identiques. Par conséquent, au moins quatre indicatifs régionaux sont nécessaires pour garantir que tous les numéros à 10 chiffres sont différents. ▲

L'exemple 9, bien qu'il ne s'agisse pas d'une application du principe généralisé des trous de pigeon, utilise de principes similaires.

EXEMPLE 9 Supposons qu'un laboratoire informatique possède 15 postes de travail et 10 serveurs. Un câble peut être utilisé pour connecter directement un poste de travail à un serveur. Pour chaque serveur, une seule connexion directe à ce serveur peut être actif à tout moment. Nous voulons garantir à tout moment un ensemble de 10 ou moins les postes de travail peuvent accéder simultanément à différents serveurs via des connexions directes. Bien que nous pourrait le faire en connectant chaque poste de travail directement à chaque serveur (en utilisant 150 connexions), quel est le nombre minimum de connexions directes nécessaires pour atteindre cet objectif?

Solution: Supposons que nous étiquetons les postes de travail $W_1, W_2, ..., W_{15}$ et les serveurs $S_1, S_2, ..., S_{10}$. De plus, supposons que nous connectons W_k à S_k pour $k = 1, 2, ..., 10$ et chacun de $W_{11}, W_{12}, W_{13}, W_{14}$ et W_{15} aux 10 serveurs. Nous avons un total de 60 connexions directes. De toute évidence, un ensemble de 10 postes de travail ou moins peut accéder simultanément à différents serveurs. Nous voyons ceci en notant que si le poste de travail W_j est inclus avec $1 \leq j \leq 10$, il peut accéder au serveur S_j, et pour chaque poste de travail W_k avec $k \geq 11$ inclus, il doit y avoir un poste de travail correspondant W_j

avec $1 \leq j \leq 10$ non inclus, donc W_k peut accéder au serveur S_j. (Cela suit parce qu'il y a moins de serveurs S_j disponibles qu'il y a de postes de travail W_j avec $1 \leq j \leq 10$ non inclus.)

Supposons maintenant qu'il y ait moins de 60 connexions directes entre les postes de travail et les serveurs. Un serveur serait alors connecté à au plus $\lfloor 59/10 \rfloor = 5$ postes de travail.(Si tous les serveurs étaient connecté à au moins six postes de travail, il y aurait au moins $6 \cdot 10 = 60$ connexions directes.) Cela signifie que les neuf serveurs restants ne sont pas suffisants pour permettre aux 10 autres postes de travail de accéder simultanément à différents serveurs. Par conséquent, au moins 60 connexions directes sont nécessaires. Il s'ensuit que 60 est la réponse. ▲

Quelques applications élégantes du principe du pigeonnier

Dans de nombreuses applications intéressantes du principe du pigeonnier, les objets à placer dans des boîtes doit être choisi de manière intelligente. Quelques-unes de ces applications seront décrites ici.

EXEMPLE 10 Pendant un mois avec 30 jours, une équipe de baseball joue au moins un match par jour, mais pas plus de 45 matchs. Montrer qu'il doit y avoir une période d'un certain nombre de jours consécutifs pendant que l'équipe doit jouer exactement 14 matchs.

Solution: Soit a_j le nombre de parties jouées le ou avant le j ème jour du mois. alors $a_1, a_2, \ldots, a_{30}$ est une séquence croissante d'entiers positifs distincts, avec $1 \leq a_j \leq 45$. Plus-plus, $un_1 + 14$, $un_2 + 14$, ..., $un_{30} + 14$ est également une séquence croissante d'entiers positifs distincts, avec $15 \leq a_j + 14 \leq 59$.

Les 60 entiers positifs $a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_{30} + 14$ sont tous inférieurs à ou égal à 59. Par conséquent, selon le principe du pigeonhole, deux de ces nombres entiers sont égaux.Parce que le les entiers a_j, $j = 1, 2, \ldots, 30$ sont tous distincts et les entiers $a_j + 14$, $j = 1, 2, \ldots, 30$ sont tous distincts, il doit y avoir des indices i et j avec $a_i = a_j + 14$. Cela signifie que exactement 14 jeux ont été joués du jour $j + 1$ au jour i. ▲

EXEMPLE 11 Montrer que parmi $n + 1$ entiers positifs ne dépassant pas $2n$, il doit y avoir un entier qui divise l'un des autres entiers.

Solution: Écrivez chacun des $n + 1$ entiers $a_1, a_2, \ldots, a_{n+1}$ comme une puissance de 2 fois un entier impair. En d'autres termes, soit $a_j = 2^{k_j} q_j$ pour $j = 1, 2, \ldots, n + 1$, où k_j est un entier non négatif et q_j est impair. Les entiers $q_1, q_2, \ldots, q_{n+1}$ sont tous des entiers positifs impairs inférieurs à $2n$. Parce que là ne sont que n entiers positifs impairs inférieurs à $2n$, il découle du principe du pigeonnier que deux des entiers $q_1, q_2, \ldots, q_{n+1}$ doit être égal. Par conséquent, il existe des entiers distincts i et j tels que $q_i = q_j$. Soit q la valeur commune de q_i et q_j. Ensuite, $a_i = 2^{k_i} q$ et $a_j = 2^{k_j} q$. Ça suit que si $k_i < k_j$, alors a_i divise a_j ; tandis que si $k_i > k_j$, alors a_j divise a_i. ▲

Une application astucieuse du principe du pigeonnier montre l'existence d'un sous-séquence décroissante d'une certaine longueur dans une séquence d'entiers distincts. Nous passons en revue certains définitions avant cette application est présentée. Supposons que $a_1, a_2, \ldots, a_N$ est une séquence de nombres réels. Une **sous** -séquence de cette séquence est une séquence de la forme $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$, où $1 \leq i_1 < i_2 < \cdots < i_m \leq N$. Par conséquent, une sous-séquence est une séquence obtenue à partir de l'original séquence en incluant certains termes de la séquence d'origine dans leur ordre d'origine, et n'incluant peut-être pas d'autres termes. Une séquence est appelée **strictement croissante** si chaque terme est plus grand que celui qui le précède, et il est appelé **strictement décroissant** si chaque terme est plus petit que le celui qui le précède.

THÉORÈME 3 Chaque séquence de $n^2 + 1$ nombres réels distincts contient une sous-séquence de longueur $n + 1$ qui augmente ou diminue strictement.

Nous donnons un exemple avant de présenter la preuve du Théorème 3.

EXEMPLE 12 La séquence 8, 11, 9, 1, 4, 6, 12, 10, 5, 7 contient 10 termes. Notez que $10 = 3^2 + 1$. Il sont quatre sous-séquences strictement croissantes de longueur quatre, à savoir 1, 4, 6, 12; 1, 4, 6, 7; 1, 4, 6, 10; et 1, 4, 5, 7. Il y a aussi une sous-séquence strictement décroissante de longueur quatre, à savoir, 11, 9, 6, 5. ▲

La preuve du théorème va maintenant être donnée.

Preuve: Soit $a_1, a_2, \ldots, a_{n^2+1}$ une suite de $n^2 + 1$ nombres réels distincts. Associer un ordre paire avec chaque terme de la séquence, à savoir, associer (i_k, d_k) au terme a_k, où i_k est le longueur de la sous-séquence croissante la plus longue commençant à a_k, et d_k est la longueur de la plus longue sous-séquence décroissante commençant à a_k.

Supposons qu'il n'y ait pas de sous-séquences croissantes ou décroissantes de longueur $n + 1$. Alors i_k et d_k sont tous deux des entiers positifs inférieurs ou égaux à n, pour $k = 1, 2, \ldots, n^2 + 1$. Par conséquent, par le règle du produit il y a n^2 paires ordonnées possibles pour (i_k, d_k). Selon le principe du pigeonnier, deux des ces $n^2 + 1$ paires ordonnées sont égales. En d'autres termes, il existe des termes a_s et a_t, avec $s < t$ tels que $i_s = i_t$ et $d_s = d_t$. Nous montrerons que cela est impossible. Parce que les termes de la les séquences sont distinctes, soit $a_s < a_t$ ou $a_s > a_t$. Si $a_s < a_t$, alors, parce que $i_s = i_t$, une augmentation une sous-séquence de longueur $i_t + 1$ peut être construite à partir de a_s, en prenant a_s suivi d'une augmentation sous-séquence de longueur i_t commençant à a_t. C'est une contradiction. De même, si $a_s > a_t$, le même le raisonnement montre que d_s doit être supérieur à d_t, ce qui est une contradiction.

Le dernier exemple montre comment le principe généralisé du trou de pigeon peut être appliqué à partie importante de la combinatoire appelée **théorie de Ramsey**, d'après le mathématicien anglais FP Ramsey. En général, la théorie de Ramsey traite de la distribution de sous-ensembles d'éléments d'ensembles.

EXEMPLE 13 Supposons que dans un groupe de six personnes, chaque paire d'individus se compose de deux amis ou deux ennemis. Montrez qu'il y a soit trois amis communs, soit trois ennemis communs dans le groupe.

Solution: Soit A l'une des six personnes. Des cinq autres personnes du groupe, il y a soit trois ou plus qui sont des amis de A, ou trois ou plus qui sont des ennemis de A. Cela découle de le principe du pigeonnier généralisé, car lorsque cinq objets sont divisés en deux ensembles, un des ensembles a au moins $\lceil 5/2 \rceil = 3$ éléments. Dans le premier cas, supposons que B, C et D soient amis de A. Si deux de ces trois individus sont amis, ces deux et A forment un groupe de trois amis communs. Sinon, B, C et D forment un ensemble de trois ennemis mutuels. La preuve dans ce dernier cas, lorsqu'il y a trois ennemis ou plus de A, procède de la même manière. ▲

Le **nombre de Ramsey** $R(m, n)$, où m et n sont des entiers positifs supérieurs ou égaux à 2, indique le nombre minimum de personnes à une fête de telle sorte qu'il y ait soit m amis mutuels ou n ennemis mutuels, en supposant que chaque paire de personnes à la fête sont des amis ou des ennemis. L'exemple 13 montre que $R(3, 3) \leq 6$. Nous concluons que $R(3, 3) = 6$ parce que dans un groupe de cinq

FRANK PLUMPTON RAMSEY (1903–1930) Frank Plumpton Ramsey, fils du président de Magdalene Le Collège de Cambridge a fait ses études aux collèges Winchester et Trinity. Après avoir obtenu son diplôme en 1923, il a été élu boursier du King's College de Cambridge, où il a passé le reste de sa vie. Ramsey fait de l'importance contributions à la logique mathématique. Ce que nous appelons maintenant la théorie de Ramsey a commencé avec sa combinatoire intelligente arguments, publiés dans le document «Sur un problème de logique formelle». Ramsey a également contribué à la théorie mathématique de l'économie. Il a été noté comme un excellent conférencier sur les fondements des mathématiques. Selon l'un de ses frères, il s'intéressait à presque tout, y compris la littérature anglaise et la politique. Ramsey était marié et avait deux filles. Sa mort à 26 ans des suites de problèmes hépatiques chroniques privé la communauté mathématique et l'Université de Cambridge d'un brillant jeune universitaire.

Épisode 426

les gens où tous les deux sont amis ou ennemis, il ne peut y avoir trois amis communs ou trois ennemis mutuels (voir exercice 26).

Il est possible de prouver certaines propriétés utiles sur les nombres de Ramsey, mais pour la plupart en partie il est difficile de trouver leurs valeurs exactes. Notez que par symétrie, on peut montrer que $R(m, n) = R(n, m)$ (voir exercice 30). Nous avons également $R(2, n) = n$ pour chaque entier positif $n \geq 2$ (voir exercice 29). Les valeurs exactes de seulement neuf nombres de Ramsey $R(m, n)$ avec $3 \leq m \leq n$ sont connu, y compris $R(4, 4) = 18$. Seules les bornes sont connues pour de nombreux autres nombres de Ramsey, y compris $R(5, 5)$, qui est connu pour satisfaire $43 \leq R(5, 5) \leq 49$. Le lecteur intéressé à apprendre Pour en savoir plus sur les numéros Ramsey, consultez [MiRo91] ou [GrRoSp90].

Des exercices

1. Montrez que dans n'importe quel ensemble de six classes, chaque généralement une fois par semaine un jour particulier de la semaine, doivent être deux qui se réunissent le même jour, en supposant qu'aucun les cours ont lieu le week-end.

2. Montrez que s'il y a 30 élèves dans une classe, alors au moins deux ont des noms de famille commençant par la même lettre.

3. Un tiroir contient une douzaine de chaussettes brunes et une douzaine de chaussettes noires chaussettes, toutes inégalées. Un homme prend des chaussettes au hasard dans le noir.

a) Combien de chaussettes doit-il retirer pour être sûr qu'il a au moins deux chaussettes de la même couleur?

b) Combien de chaussettes doit-il retirer pour être sûr qu'il a au moins deux chaussettes noires?

4. Un bol contient 10 boules rouges et 10 boules bleues. Une femme sélectionne les balles au hasard sans les regarder.

a) Combien de balles doit-elle sélectionner pour être sûre d'avoir au moins trois boules de la même couleur?

b) Combien de balles doit-elle sélectionner pour être sûre d'avoir au moins trois boules bleues?

5. Montrez que parmi tout groupe de cinq (pas nécessairement entiers), il y en a deux avec le même reste lorsqu'il est divisé par 4.

6. Soit d un entier positif. Montrez que parmi tout groupe de $d + 1$ (pas nécessairement consécutifs) entiers il y a deux avec exactement le même reste lorsqu'ils sont divisés par d .

7. Soit n un entier positif. Montrez que dans n'importe quel ensemble de n entiers consécutifs il y a exactement un divisible par n .

8. Montrer que si f est une fonction de S à T , où S et T sont des ensembles finis avec $|S| > |T|$, alors il y a des éléments s_1 et s_2 dans S tels que $f(s_1) = f(s_2)$, ou en d'autres termes, f n'est pas un à un.

9. Quel est le nombre minimum d'étudiants, dont chacun vient de l'un des 50 États, qui doivent être inscrits dans une université pour garantir qu'il y a au moins 100 qui viennent du même état?

∗ **10.** Soit (x_i, y_i) , $i = 1, 2, 3, 4, 5$, un ensemble de cinq points distincts avec des coordonnées entières dans le plan xy . Montrez que le milieu de la ligne joignant au moins une paire de ces points a des coordonnées entières.

∗ **11.** Soit (x_i, y_i, z_i) , $i = 1, 2, 3, 4, 5, 6, 7, 8, 9$, un ensemble de neuf points distincts avec des coordonnées entières dans l' espace xyz . Spectacle que le milieu d'au moins une paire de ces points a coordonnées entières.

12. Combien de paires ordonnées d'entiers (a, b) sont nécessaire pour garantir qu'il y a deux paires ordonnées (a_1, b_1) et (a_2, b_2) de telle sorte que *un* $_1$ **mod** 5 = *un* $_2$ **mod** 5 et b_1 **mod** $5 = b_2$ **mod** 5?

13. a) Montrer que si cinq nombres entiers sont sélectionnés dans le premier huit entiers positifs, il doit y en avoir une paire entiers avec une somme égale à 9.

b) La conclusion de la partie (a) est-elle vraie si quatre entiers sont sélectionné plutôt que cinq?

14. a) Montrer que si sept entiers sont sélectionnés dans le premier 10 entiers positifs, il doit y avoir au moins deux paires de ces entiers avec la somme 11.

b) La conclusion de la partie (a) est-elle vraie si six entiers sont sélectionné plutôt que sept?

15. Combien de numéros doivent être sélectionnés dans l'ensemble $\{1, 2, 3, 4, 5, 6\}$ pour garantir qu'au moins une paire de ces les nombres totalisent jusqu'à 7?

16. Combien de numéros doivent être sélectionnés dans l'ensemble $\{1, 3, 5, 7, 9, 11, 13, 15\}$ pour garantir qu'au moins une paire de ces nombres totalisent 16?

17. Une entreprise stocke des produits dans un entrepôt. Bacs de stockage dans cet entrepôt sont spécifiés par leur allée, leur emplacement dans l'allée et l'étagère. Il y a 50 allées, 85 horizontales emplacements dans chaque allée, et 5 étagères dans tout le magasin maison. Quel est le moins de produits de l'entreprise peut avoir de sorte qu'au moins deux produits doivent être stockés dans le même bac?

18. Supposons qu'il y ait neuf élèves dans une matière discrète cours de matiques dans un petit collège.

a) Montrer que la classe doit avoir au moins cinq étudiants masculins ou au moins cinq étudiantes.

b) Montrer que la classe doit avoir au moins trois étudiants masculins ou au moins sept étudiantes.

19. Supposons que chaque élève d'une classe de mathématiques discrète de 25 étudiants est un étudiant de première année, un étudiant en deuxième année ou un junior.

a) Montrer qu'il y a au moins neuf étudiants de première année, au moins neuf étudiants de deuxième année, ou au moins neuf juniors dans la classe.

b) Montrer qu'il y a au moins trois étudiants de première année, au moins 19 étudiants de deuxième année, ou au moins cinq juniors dans la classe.

20. Trouver une sous-séquence croissante de longueur maximale et une sous-séquence décroissante de longueur maximale dans la par conséquent 22, 5, 7, 2, 23, 10, 15, 21, 3, 17.

21. Construisez une séquence de 16 entiers positifs qui n'a pas augmentation ou diminution de la sous-séquence de cinq termes.

22. Montrer que s'il y a 101 personnes de différentes hauteurs debout, il est possible de trouver 11 personnes dans le afin qu'ils se tiennent dans la ligne avec des hauteurs qui sont soit en augmentation soit en diminution.

∗ **23.** Montrez que chaque fois que 25 filles et 25 garçons sont assis autour d'une table circulaire, il y a toujours une personne à la fois dont les voisins sont des garçons.

∗∗ **24.** Supposons que 21 filles et 21 garçons entrent en Concours ics. De plus, supposons que chaque participant résout au plus six questions, et pour chaque paire garçon-fille, il y a au moins une question qu'ils ont tous deux résolue. Spectacle qu'il y a une question qui a été résolue par au moins trois filles et au moins trois garçons.

∗ **25.** Décrire un algorithme en pseudocode pour produire le la plus forte augmentation ou diminution de la sous-séquence d'une d'entiers distincts.

Nicole a fait, qu'il devait y avoir deux Parisiens avec le même nombre de poils sur la tête. Utilisez ensuite le générateur principe de trou de pige harmonisé pour montrer qu'il devait y avoir au moins cinq Parisiens à cette époque avec le même numéro de poils sur la tête.

34. En supposant que personne n'a plus de 1 000 000 de cheveux sur le chef de toute personne et que la population de New York City était 8 008 278 en 2010, montrer qu'il devait y avoir à au moins neuf personnes à New York en 2010 avec le même nombre de poils sur la tête.

35. Il y a 38 périodes différentes pendant lesquelles les cours dans une université peut être programmé. S'il y a 677 différents classes, combien de salles différentes seront nécessaires?

36. Un réseau informatique comprend six ordinateurs. Chaque com- ordinateur est directement connecté à au moins un des autres puters. Montrez qu'il y a au moins deux ordinateurs dans le réseau directement connecté au même numéro d'autres ordinateurs.

37. Un réseau informatique comprend six ordinateurs. Chaque com- l'ordinateur est directement connecté à zéro ou plus de l'autre des ordinateurs. Montrer qu'il y a au moins deux ordinateurs dans du réseau qui sont directement connectés au même numéro nombre d'autres ordinateurs. [*Indice:* il est impossible d'avoir un ordinateur relié à aucun des autres et un ordinateur

26. Montrez que dans un groupe de cinq personnes (où deux personnes sont soit des amis, soit des ennemis), il n'y a pas nécessairement trois amis communs ou trois ennemis communs.

27. Montrez que dans un groupe de 10 personnes (où deux personnes sont des amis ou des ennemis), il y a soit trois mu- amis ou quatre ennemis mutuels, et il y a soit trois ennemis communs ou quatre amis communs.

28. Utilisez l'exercice 27 pour montrer que parmi tout groupe de 20 personnes (où deux personnes sont des amis ou des personnes mies), il y a soit quatre amis ou quatre amis ennemis.

29. Montrer que si n est un entier avec $n \geq 2$, alors le Ramsey le nombre $R(2, n)$ est égal à n . (Rappelons que les numéros de Ramsey ont été examinés après l'exemple 13 de la section 6.2.)

30. Montrer que si m et n sont des entiers avec $m \geq 2$ et $n \geq 2$, alors les nombres de Ramsey $R(m, n)$ et $R(n, m)$ sont égaux. (Rappelons que les nombres de Ramsey ont été discutés après examen ple 13 dans la section 6.2.)

31. Montrez qu'il y a au moins six personnes en Californie (pop- tion: 37 millions) avec les trois mêmes initiales qui étaient né le même jour de l'année (mais pas nécessairement la même année). Supposons que tout le monde ait trois initiales.

32. Montrer que s'il y a 100 000 000 de salariés dans le États-Unis qui gagnent moins de 1 000 000 de dollars (mais au moins un sou), alors il y en a deux qui ont gagné exactement la même somme d'argent, au centime, l'an dernier.

33. Au XVIIe siècle, il y avait plus de 800 000 habitants itinérants de Paris. À l'époque, on croyait que personne n'avait plus de 200 000 cheveux sur la tête. En supposant que ces les chiffres sont corrects et que tout le monde a au moins un cheveu sur la tête (c'est-à-dire que personne n'est complètement chauve), utilisez le principe du pigeonnier à montrer, comme l'écrivain français Pierre

lié à tous les autres.]

38. Trouvez le moins de câbles nécessaires pour connecter huit ordinateurs à quatre imprimantes pour garantir que pour chaque choix de quatre des huit ordinateurs, ces quatre ordinateurs les puters peuvent accéder directement à quatre imprimantes différentes. Justifier Ta Réponse.

39. Trouvez le moins de câbles nécessaires pour connecter 100 ordinateurs à 20 imprimantes pour garantir que chaque sous-ensemble 2 20 ordinateurs peuvent accéder directement à 20 imprimantes différentes. (Ici, les hypothèses sur les câbles et les ordinateurs sont comme dans l'exemple 9.) Justifiez votre réponse.

∗ **40.** Prouvez que lors d'une fête où il y a au moins deux personnes, il y a deux personnes qui connaissent le même nombre d'autres des gens là.

41. Un lutteur d'armes est le champion pour une période de 75 heures. (Ici, par une heure, nous entendons une période à partir d'un heure exacte, comme 13 heures, jusqu'à l'heure suivante.) Le bras Le lutteur avait au moins un match par heure, mais pas plus de 125 matchs au total. Montrer qu'il y a une période de heures utiles pendant lesquelles le lutteur de bras avait exactement 24 allumettes.

∗ **42.** L'énoncé de l'exercice 41 est-il vrai si 24 est remplacé par

a) 2? **b)** 23? **c)** 25? **d)** 30?

43. Montrer que si f est une fonction de S à T , où S et T sont ensembles finis non vides et $m = \lceil |S| / |T| \rceil$, alors il y a à moins m éléments de S mappées à la même valeur de T . Cette est, montrer qu'il existe des éléments distincts $s_1, s_2, ..., s_m$ de S tel que $f(s_1) = f(s_2) = \cdots = f(s_m)$.

44. Il y a 51 maisons dans une rue. Chaque maison a une adresse entre 1000 et 1099 inclus. Montrez qu'au moins deux les maisons ont des adresses qui sont des entiers consécutifs.

∗ **45.** Soit x un nombre irrationnel. Montrez que pour certains positifs entier j ne dépassant pas l'entier positif n , l'absolu valeur de la différence entre jx et l'entier le plus proche à jx est inférieur à $1/n$.

46. Soit $n_1, n_2, ..., n_t$ des entiers positifs. Montrez que si $n_1 + n_2 + \cdots + n_t - t + 1$ objets sont placés dans t cases, puis pour certains i, $i = 1, 2, ..., t$, la i ème case con- contient au moins n_i objets.

∗ **47.** Une preuve alternative du Théorème 3 basée sur le Le principe du trou de pige standardisé est décrit dans cet exercice. le la notation utilisée est la même que celle utilisée dans la preuve du texte.

a) Supposons que $i_k \leq n$ pour $k = 1, 2, ..., n^2 + 1$. Utilisez la principe généralisé des trous de pigeon pour montrer sont $n + 1$ termes $a_{k_1}, a_{k_2}, ..., a_{k_{n+1}}$ avec $i_{k_1} = i_{k_2} = \cdots = i_{k_{n+1}}$, où $1 \leq k_1 < k_2 < \cdots < k_{n+1}$.

b) Montrer que $a_{k_j} > a_{k_{j+1}}$ pour $j = 1, 2, ..., n$. [*Indice:* As- supposons que $a_{k_j} < a_{k_{j+1}}$, et montrent que cela implique que $i_{k_j} > i_{k_{j+1}}$, ce qui est une contradiction.]

c) Utilisez les parties (a) et (b) pour montrer que s'il n'y a pas sous-séquence de longueur $n + 1$, alors il doit y avoir une sous-séquence décroissante de cette longueur.

Permutations et combinaisons

introduction

De nombreux problèmes de comptage peuvent être résolus en trouvant le nombre de façons d'organiser un nombre d'éléments distincts d'un ensemble d'une taille particulière, où l'ordre de ces éléments importe. De nombreux autres problèmes de comptage peuvent être résolus en trouvant le nombre de façons de sélectionner un nombre particulier d'éléments d'un ensemble d'une taille particulière, où l'ordre des éléments sélectionné n'a pas d'importance. Par exemple, de combien de façons pouvons-nous sélectionner trois étudiants un groupe de cinq étudiants pour faire la queue pour une photo?Combien de comités différents de trois les étudiants peuvent être formés à partir d'un groupe de quatre étudiants?Dans cette section, nous développerons des méthodes pour répondre à de telles questions.

Permutations

Nous commençons par résoudre la première question posée dans l'introduction de cette section, ainsi que les des questions.

EXEMPLE 1 De combien de façons pouvons-nous sélectionner trois étudiants dans un groupe de cinq étudiants pour Une image? De combien de façons pouvons-nous organiser ces cinq étudiants en ligne pour une photo?

Solution: Tout d'abord, notez que l'ordre dans lequel nous sélectionnons les étudiants est important. Il y a cinq façons pour sélectionner le premier élève à se tenir au début de la ligne.Une fois cet étudiant sélectionné, il existe quatre façons de sélectionner le deuxième élève de la ligne.Après les premier et deuxième étudiants ont été sélectionnés, il existe trois façons de sélectionner le troisième élève de la lignePar le produit règle, il y a $5 \cdot 4 \cdot 3 = 60$ façons de sélectionner trois étudiants parmi un groupe de cinq étudiants en ligne pour une photo.

Pour organiser les cinq étudiants en ligne pour une image, nous sélectionnons le premier étudiant de cinq façons, le deuxième de quatre façons, le troisième de trois façons, le quatrième de deux façons et le cinquième en un façon. Par conséquent, il existe $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ façons d'organiser les cinq élèves en ligne pour Une image. ▲

L'exemple 1 illustre comment les arrangements ordonnés d'objets distincts peuvent être comptés.Cela conduit à une certaine terminologie.

Une **permutation** d'un ensemble d'objets distincts est une disposition ordonnée de ces objets. Nous nous intéressons également aux arrangements ordonnés de certains éléments d'un ensemble.Un ordre la disposition des r éléments d'un ensemble est appelée ***r*- permutation** .

EXEMPLE 2 Soit $S = \{1, 2, 3\}$. L'agencement ordonné 3, 1, 2 est une permutation de S . L'arrangement ordonné 3, la figure 2 est un 2-permutation de S . ▲

Le nombre de r- permutations d'un ensemble avec n éléments est noté $P(n, r)$. Nous pouvons trouver $P(n, r)$ *en* utilisant la règle du produit.

EXEMPLE 3 Soit $S = \{a, b, c\}$. Les 2 permutations de S sont les arrangements ordonnés a, b ; a, c ; b, a ; b, c ; c, a ; et c, b . Par conséquent, il y a six 2 permutations de cet ensemble avec trois éléments. Il y a toujours six permutations à 2 d'un ensemble à trois éléments. Là sont trois façons de choisir le premier élément de l'arrangement.Il existe deux façons de choisir deuxième élément de l'arrangement, car il doit être différent du premier élément.Par conséquent, par la règle du produit, nous voyons que $P(3, 2) = 3 \cdot 2 = 6$. le premier élément.Par la règle du produit, il s'ensuit que $P(3, 2) = 3 \cdot 2 = 6$. ▲

Nous utilisons maintenant la règle du produit pour trouver une formule pour $P(n, r)$ chaque fois que n et r sont des entiers positifs avec $1 \leq r \leq n$.

THÉORÈME 1 Si n est un entier positif et r est un entier avec $1 \leq r \leq n$, alors il y a

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r- permutations d'un ensemble avec n éléments distincts.

Preuve: Nous utiliserons la règle du produit pour prouver que cette formule est correcte.Le premier élément du la permutation peut être choisie de n façons car il y a n éléments dans l'ensemble. Il y a $n - 1$ façons de choisir le deuxième élément de la permutation, car il reste $n - 1$ éléments dans l'ensemble après avoir utilisé l'élément choisi pour la première position.De même, il existe $n - 2$ façons pour choisir le troisième élément, et ainsi de suite, jusqu'à ce qu'il y ait exactement $n - (r - 1) = n - r + 1$ façons de choisissez le r e élément. Par conséquent, selon la règle du produit, il existe

$$n(n-1)(n-2)\cdots(n-r+1)$$

r- permutations de l'ensemble.

Notez que $P(n, 0) = 1$ chaque fois que n est un entier non négatif car il y en a exactement un façon de commander zéro éléments.Autrement dit, il y a exactement une liste sans éléments, à savoir la liste vide.

Nous énonçons maintenant un corollaire utile du théorème 1.

COROLLARY 1 Si n et r sont des entiers avec $0 \leq r \leq n$, alors $P(n, r) = \dfrac{n!}{(n-r)!}$.

Preuve: Lorsque n et r sont des entiers avec $1 \leq r \leq n$, par le théorème 1 nous avons

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

Car $\dfrac{n!}{(n-0)!} = \dfrac{n!}{n!} = 1$ chaque fois que n est un entier non négatif, nous voyons que la formule

$P(n, r) = \frac{n!}{(n-r)!}$ est également valable lorsque $r = 0$.

Par le théorème 1, nous savons que si n est un entier positif, alors $P(n, n) = n!$. Nous illustrerons ce résultat avec quelques exemples.

EXEMPLE 4 De combien de façons existe-t-il pour sélectionner un gagnant du premier prix, un gagnant du deuxième prix et un troisième prix gagnant de 100 personnes différentes qui ont participé à un concours?

Solution: Parce qu'il importe quelle personne remporte quel prix, le nombre de façons de choisir le trois gagnants est le nombre de sélections commandées de trois éléments parmi un ensemble de 100 éléments, c'est-à-dire le nombre de 3 permutations d'un ensemble de 100 éléments.Par conséquent, le la réponse est

$P(100, 3) = 100 \cdot 99 \cdot 98 = 970, 200$. ▲

EXEMPLE 5 Supposons qu'il y ait huit coureurs dans une course. Le vainqueur reçoit une médaille d'or, le deuxième le finisseur en place reçoit une médaille d'argent, et le troisième finisseur reçoit une médaille de bronze.Comment il existe de nombreuses façons d'attribuer ces médailles, si tous les résultats possibles de la course se produire et il n'y a pas de liens?

Solution: Le nombre de façons différentes d'attribuer les médailles est le nombre de 3 permutations d'un ensemble à huit éléments. Par conséquent, il existe $P(8, 3) = 8 \cdot 7 \cdot 6 = 336$ façons possibles d'attribuer les médailles. ▲

EXEMPLE 6 Supposons qu'une vendeuse doive visiter huit villes différentes.Elle doit commencer son voyage dans un ville, mais elle peut visiter les sept autres villes dans l'ordre qu'elle souhaite.Combien de commandes possibles la vendeuse peut-elle utiliser pour visiter ces villes?

Solution: Le nombre de chemins possibles entre les villes est le nombre de permutations de sept éléments, car la première ville est déterminée, mais les sept autres peuvent être commandés arbitrairement. Par conséquent, il y en a $7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ voies pour la vendeuse de choisir sa tournée. Si, par exemple, la vendeuse souhaite trouver le chemin entre les villes avec une distance minimale, et elle calcule la distance totale pour chaque chemin possible, elle doit considérez un total de 5040 chemins! ▲

EXEMPLE 7 Combien de permutations des lettres *ABCDEFGH* contiennent la chaîne *ABC* ?

Solution: Parce que les lettres *ABC* doivent apparaître comme un bloc, nous pouvons trouver la réponse en trouvant le nombre de permutations de six objets, à savoir le bloc *ABC* et les lettres individuelles D, E, F, G, et H. Parce que ces six objets peuvent apparaître dans n'importe quel ordre, il y en a $6! = 720$ permutations des lettres *ABCDEFGH* dans lesquelles *ABC* apparaît comme un bloc. ▲

Combinaisons

Nous tournons maintenant notre attention vers le comptage des sélections non ordonnées d'objets.Nous commençons par résoudre un question posée dans l'introduction de cette section du chapitre.

EXEMPLE 8 Combien de comités différents de trois étudiants peuvent être formés à partir d'un groupe de quatre étudiants?

Solution: pour répondre à cette question, il suffit de trouver le nombre de sous-ensembles à trois éléments de l'ensemble contenant les quatre étudiants.Nous voyons qu'il existe quatre sous-ensembles de ce type, un pour chacun des quatre étudiants, car le choix de trois étudiants revient à choisir l'un des quatre étudiants à exclure du groupe.Cela signifie qu'il existe quatre façons de choisir trois étudiants pour le comité, où l'ordre dans lequel ces étudiants sont choisis ne correspond pas matière. ▲

L'exemple 8 montre que de nombreux problèmes de comptage peuvent être résolus en trouvant le nombre de sous-ensembles d'une taille particulière d'un ensemble avec n éléments, où n est un entier positif.

Une ***r*- combinaison** d'éléments d'un ensemble est une sélection non ordonnée d'éléments r de l'ensemble. Ainsi, une combinaison r est simplement un sous-ensemble de l'ensemble avec r éléments.

EXEMPLE 9 Soit S l'ensemble $\{1, 2, 3, 4\}$. Ensuite, $\{1, 3, 4\}$ est un 3-combinaison de S. (Notez que $\{4, 1, 3\}$ est le même combinaison de 3 que $\{1, 3, 4\}$, car l'ordre dans lequel les éléments d'un ensemble sont répertoriés ne pas important.) ▲

Le nombre de r -combinaisons d'un ensemble avec n éléments distincts est noté $C(n, r)$. Remarque que $C(n, r)$ est également désigné par $\binom{n}{r}$ et est appelé un **coefficient binomial**. Nous apprendrons où cette terminologie provient de la section 6.4.

EXEMPLE 10 On voit que $C(4, 2) = 6$, car les 2 combinaisons de $\{a, b, c, d\}$ sont les six sous-ensembles $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$ et $\{c, d\}$. ▲

Nous pouvons déterminer le nombre de r -combinaisons d'un ensemble avec n éléments en utilisant la formule pour le nombre de r- permutations d'un ensemble. Pour ce faire, notez que les r- permutations d'un ensemble peuvent être obtenu en formant d'abord des combinaisons r puis en ordonnant les éléments dans ces combinaisons. La preuve du théorème 2, qui donne la valeur de $C(n, r)$, est basée sur cette observation.

THÉORÈME 2 Le nombre de r -combinaisons d'un ensemble avec n éléments, où n est un entier non négatif et r est un entier avec $0 \leq r \leq n$, égal à

$$C(n, r) = \frac{n!}{r!\,(n-r)!}.$$

Preuve: Les permutations $P(n, r)$ r de l'ensemble peuvent être obtenues en formant le $C(n, r)$ r -combinaisons de l'ensemble, puis ordonner les éléments dans chaque r -combinaison, qui peut être fait de façon $P(r, r)$. Par conséquent, selon la règle du produit,

$$P(n, r) = C(n, r) \cdot P(r, r).$$

Ceci implique que

$$C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!/(n-r)!}{r!/(r-r)!} = \frac{n!}{r!\,(n-r)!}.$$

Nous pouvons également utiliser la règle de division pour compter pour construire une preuve de ce théorème. Parce que le l'ordre des éléments dans une combinaison n'a pas d'importance et il existe $P(r, r)$ façons de *ranger les* éléments dans une r- combinaison de n éléments, chacune des $C(n, r)$ r- combinaisons d'un ensemble avec n éléments correspond exactement à $P(r, r)$ r- permutations. Par conséquent, selon la règle de division, $C(n, r) = \frac{P(n, r)}{P(r, r)}$, ce qui implique comme précédemment que $C(n, r) = \frac{n!}{r!\,(n-r)!}$.

La formule du théorème 2, bien qu'explicite, n'est pas utile lorsque $C(n, r)$ est calculé pour grandes valeurs de n et r. Les raisons en sont qu'il est pratique de calculer les valeurs exactes des factorielles exactement uniquement pour les petites valeurs entières, et lorsque l'arithmétique à virgule flottante est utilisée, la formule Le théorème 2 peut produire une valeur qui n'est pas un entier. Lors du calcul de $C(n, r)$, notez d'abord que quand nous annulons $(n - r)!$ à partir du numérateur et du dénominateur de l'expression pour $C(n, r)$ dans le théorème 2, on obtient

$$C(n, r) = \frac{n!}{r!\,(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}.$$

Par conséquent, pour calculer $C(n, r)$, vous pouvez annuler tous les termes de la plus grande factorielle dans le dénominateur du numérateur et du dénominateur, puis multipliez tous les termes qui n'annulent pas dans le numérateur et enfin diviser par la plus petite factorielle dans le dénominateur.[En faisant ce calcul à la main, plutôt qu'à la machine, il est également utile de tenir compte des facteurs dans le numérateur $n(n-1)\cdots(n-r+1)$ et dans le dénominateur $r!$.] Notez que beaucoup les calculatrices ont une fonction intégrée pour $C(n, r)$ qui peut être utilisée pour des valeurs relativement petites de n et r et de nombreux programmes de calcul peuvent être utilisés pour trouver $C(n, r)$. [Ces fonctions peuvent être appelé *choisir* (n, k) ou *binom* (n, k)].

L'exemple 11 illustre comment $C(n, k)$ est calculé lorsque k est relativement petit par rapport à n et quand k est proche de n. Il illustre également une identité clé dont jouissent les nombres $C(n, k)$.

EXEMPLE 11 Combien de mains de poker de cinq cartes peuvent être distribuées à partir d'un jeu standard de 52 cartes? Aussi, comment de nombreuses façons de sélectionner 47 cartes dans un jeu standard de 52 cartes?

Solution: parce que l'ordre dans lequel les cinq cartes sont distribuées à partir d'un jeu de 52 cartes ne importe, il y a

$$C(52, 5) = \frac{52!}{5!\,47!}$$

différentes mains de cinq cartes qui peuvent être distribuées. Pour calculer la valeur de $C(52, 5)$, divisez d'abord le numérateur et dénominateur par 47! obtenir

$$C(52, 5) = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}.$$

Cette expression peut être simplifiée en divisant d'abord le facteur 5 du dénominateur par le facteur 50 dans le numérateur pour obtenir un facteur 10 dans le numérateur, puis en divisant le facteur 4 dans le dénominateur dans le facteur 48 au numérateur pour obtenir un facteur de 12 au numérateur, puis diviser le facteur 3 du dénominateur par le facteur 51 du numérateur pour obtenir un facteur de 17 au numérateur, et enfin, en divisant le facteur 2 du dénominateur par le facteur 52 en le numérateur pour obtenir un facteur de 26 au numérateur. Nous constatons que

$$C(52, 5) = 26 \cdot 17 \cdot 10 \cdot 49 \cdot 12 = 2{,}598{,}960.$$

Par conséquent, 2 598 960 mains de poker différentes de cinq cartes peuvent être distribuées jeu standard de 52 cartes.

Notez qu'il existe

$$C(52, 47) = \frac{52!}{47!\,5!}$$

différentes façons de sélectionner 47 cartes dans un jeu standard de 52 cartes. Nous n'avons pas besoin de calculer cette valeur car $C(52, 47) = C(52, 5)$. (Seul l'ordre des facteurs 5! Et 47! Est différent dans les dénominateurs des formules de ces quantités.) Il s'ensuit qu'il y a également 2 598 960 différentes façons de sélectionner 47 cartes dans un jeu standard de 52 cartes. ▲

Dans l'exemple 11, nous avons observé que $C(52, 5) = C(52, 47)$. Ceci est un cas particulier de l'utile identité pour le nombre de combinaisons r d'un ensemble donné dans le corollaire 2.

COROLLARY 2 Soit n et r des entiers non négatifs avec $r \leq n$. Alors $C(n, r) = C(n, n-r)$.

Preuve: du théorème 2, il s'ensuit que

$$C(n, r) = \frac{n!}{r!\,(n-r)!}$$

et

$$C\,(n,\,n-r) = \frac{n\,!}{(n-r)\,!\,[\,n-(n-r)\,]!} = \frac{n\,!}{(n-r)\,!\,r\,!}\,.$$

Par conséquent, $C\,(n,\,r) = C\,(n,\,n-r)$.

Nous pouvons également prouver le corollaire 2 sans compter sur la manipulation algébrique.Au lieu de cela, nous pouvons utiliser une preuve combinatoire. Nous décrivons ce type important de preuve dans la définition 1.

DÉFINITION 1 Une *preuve combinatoire* d'une identité est une preuve qui utilise des arguments de comptage pour prouver que les deux côtés de l'identité comptent les mêmes objets mais de manières différentes ou une preuve basée sur en montrant qu'il y a une bijection entre les ensembles d'objets comptés par les deux côtés de l'identité. Ces deux types de preuves sont appelées*preuves à double comptage* et *preuves bijectives* , respectivement.

De nombreuses identités impliquant des coefficients binomiaux peuvent être prouvées à l'aide de preuves combinatoires.nous montrer maintenant comment prouver le corollaire 2 en utilisant une preuve combinatoire.Nous fournirons à la fois un double une preuve de comptage et une preuve bijective, toutes deux basées sur la même idée de base.

Preuves combinatoires sont presque toujours beaucoup plus court et fournir plus des idées que des preuves basé sur l'algèbre manipulation.

Preuve: Nous utiliserons une preuve bijective pour montrer que$C\,(n,\,r) = C\,(n,\,n-r)$ pour tous les entiers n et r avec $0 \leq r \leq n$. Supposons que S soit un ensemble avec n éléments. La fonction qui mappe un sous-ensemble A de S à $\bar{A}$ est une bijection entre des sous-ensembles de$S$ avec r éléments et des sous-ensembles avec$n-r$ éléments (comme le lecteur devrait vérifier). L'identité $C\,(n,\,r) = C\,(n,\,n-r)$ suit parce que lorsqu'il y a est une bijection entre deux ensembles finis, les deux ensembles doivent avoir le même nombre d'éléments.

Alternativement, nous pouvons reformuler cet argument comme une preuve de double comptage.Par définition, le nombre de sous-ensembles de$S$ avec r éléments est égal à$C\,(n,\,r)$. Mais chaque sous-ensemble A de S est également déterminée en spécifiant les éléments ne sont pas dans$A$, et sont donc en$\bar{A}$. Parce que le complément d'un sous-ensemble de$S$ avec r éléments a $n-r$ éléments, il y a aussi $C\,(n,\,n-r)$ sous-ensembles de S avec des éléments r . Il s'ensuit que $C\,(n,\,r) = C\,(n,\,n-r)$.

EXEMPLE 12 De combien de façons existe-t-il pour sélectionner cinq joueurs d'une équipe de 10 joueurs de tennis un match dans une autre école?

Solution: La réponse est donnée par le nombre de 5 combinaisons d'un ensemble de 10 éléments.Par Théorème 2, le nombre de ces combinaisons est

$$C\,(10\,,\,5\,) = \frac{\text{dix!}}{5!\;5!} = 252\,.$$ ▲

EXEMPLE 13 Un groupe de 30 personnes a été formé comme astronautes pour effectuer la première mission vers Mars.Comment il existe de nombreuses façons de sélectionner un équipage de six personnes pour cette mission (en supposant que membres ont le même emploi)?

Solution: Le nombre de façons de sélectionner un équipage de six personnes dans le groupe de 30 personnes est le nombre de 6 combinaisons d'un ensemble de 30 éléments, car l'ordre dans lequel ces personnes sont choisies n'a pas d'importance. D'après le théorème 2, le nombre de ces combinaisons est

$$C\,(30\,,\,6\,) = \frac{30!}{6!\;24!} = \frac{30\cdot 29\cdot 28\cdot 27\cdot 26\cdot 25}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 593\,,\,775\,.$$ ▲

EXEMPLE 14 Combien de chaînes de bits de longueur$n$ contiennent exactement r 1s?

Solution: les positions de$r$ 1s dans une chaîne de bits de longueur$n$ forment une r- combinaison de l'ensemble $\{1\,,\,2\,,\,3\,,\,...,\,n\,\}$. Par conséquent, il existe des chaînes de bits $C\,(n,\,r)$ de longueur n qui contiennent exactement r 1s. ▲

EXEMPLE 15 Supposons qu'il y ait 9 professeurs dans le département de mathématiques et 11 dans l'ordinateur département des sciences. Combien de façons existe-t-il pour sélectionner un comité pour développer un cours de mathématiques dans une école si le comité doit être composé de trois membres du corps professoral de la département de mathématiques et quatre du département d'informatique?

Solution: selon la règle du produit, la réponse est le produit du nombre de 3 combinaisons de un ensemble avec neuf éléments et le nombre de 4 combinaisons d'un ensemble avec 11 éléments.Par Théorème 2, le nombre de façons de sélectionner le comité est

$$C(9,3)\cdot C(11,4)=\frac{9!}{3!\,6!}\cdot\frac{11!}{4!\,7!}=84\cdot 330=27,720.$$

▲

Des exercices

1. Énumérez toutes les permutations de $\{a, b, c\}$.

2. Combien de permutations différentes y a-t-il dans l'ensemble $\{a, b, c, d, e, f, g\}$?

3. Combien de permutations de $\{a, b, c, d, e, f, g\}$ se terminent par *un* ?

4. Soit $S = \{1, 2, 3, 4, 5\}$.

a) Liste tous les 3 permutations de S.

b) Liste tous les 3 combinaisons de S.

5. Trouvez la valeur de chacune de ces quantités.

a) $P(6,3)$ **b)** $P(6,5)$
c) $P(8,1)$ **d)** $P(8,5)$
e) $P(8,8)$ **f)** $P(10,9)$

6. Trouvez la valeur de chacune de ces quantités.

a) $C(5,1)$ **b)** $C(5,3)$
c) $C(8,4)$ **d)** $C(8,8)$
e) $C(8,0)$ **f)** $C(12,6)$

7. Trouvez le nombre de 5 permutations d'un ensemble de neuf el- ements.

8. Dans combien d'ordres différents cinq coureurs peuvent-ils terminer un course si aucune égalité n'est autorisée?

9. Combien de possibilités existe-t-il pour la victoire, la place et afficher (première, deuxième et troisième) positions dans une course de chevaux avec 12 chevaux si tous les ordres d'arrivée sont possibles?

10. Il y a six candidats différents pour le poste de gouverneur d'un État. Dans combien d'ordres différents les noms des les documents doivent-ils être imprimés sur un bulletin de vote?

11. Combien de chaînes de bits de longueur 10 contiennent

a) exactement quatre 1?
b) au plus quatre 1?
c) au moins quatre 1?
d) un nombre égal de 0 et de 1?

12. Combien de chaînes de bits de longueur 12 contiennent

a) exactement trois 1?
b) au plus trois 1?
c) au moins trois 1?
d) un nombre égal de 0 et de 1?

13. Un groupe comprend n hommes et n femmes. Combien de façons sont là pour organiser ces gens dans une rangée si les hommes et les femmes alternent?

14. De combien de façons un ensemble de deux entiers positifs peut-il que 100 soient choisis?

15. De combien de façons un ensemble de cinq lettres peut-il être sélectionné de l'alphabet anglais?

16. Combien de sous-ensembles avec un nombre impair d'éléments un ensemble avec 10 éléments ont?

17. Combien de sous-ensembles de plus de deux éléments un ensemble avec 100 éléments ont?

18. Une pièce est lancée huit fois où chaque flip arrive têtes ou queues. Combien de résultats possibles

a) y en a-t-il au total?
b) contient exactement trois têtes?
c) contient au moins trois têtes?
d) contiennent le même nombre de têtes et de queues?

19. Une pièce est retournée 10 fois où chaque flip arrive soit Pile ou face. Combien de résultats possibles

a) y en a-t-il au total?
b) contient exactement deux têtes?
c) contient au plus trois queues?
d) contiennent le même nombre de têtes et de queues?

20. Combien de chaînes de bits de longueur 10 ont

a) exactement trois 0?
b) plus de 0 que de 1?
c) au moins sept 1?
d) au moins trois 1?

21. Combien de permutations des lettres *ABCDEFG* con- tain

a) la chaîne *BCD* ?
b) la chaîne *CFGA* ?
c) les cordes *BA* et *GF* ?
d) les chaînes *ABC* et *DE* ?
e) les chaînes *ABC* et *CDE* ?
f) les chaînes *CBA* et *BED* ?

22. Combien de permutations des lettres *ABCDEFGH* con- tain

a) la chaîne *ED* ?
b) la chaîne *CDE* ?
c) les cordes *BA* et *FGH* ?
d) les chaînes *AB* , *DE* et *GH* ?
e) les chaînes *CAB* et *BED* ?
f) les chaînes *BCA* et *ABF* ?

23. Combien de moyens existe-t-il pour huit hommes et cinq femmes de se tenir en ligne de sorte qu'il n'y ait pas deux femmes à côté de chaque autre? [*Indice:* positionnez d'abord les hommes, puis considérez positions possibles pour les femmes.]

24. Combien de façons existe-t-il pour 10 femmes et six hommes de se tenir en ligne de sorte qu'il n'y ait pas deux hommes à côté de chacun autre? [*Indice:* positionnez d'abord les femmes, puis considérez

28. Un professeur écrit 40 mathématiques discrètes vrai / faux des questions. Parmi les déclarations de ces questions, 17 sont vrai. Si les questions peuvent être positionnées dans n'importe quel ordre, comment de nombreuses réponses différentes sont-elles possibles?

∗ **29.** Combien de 4 permutations des entiers positifs non ex- ceeding 100 contient trois entiers consécutifs k, $k+1$, $k+2$, dans le bon ordre

a) où ces entiers consécutifs peuvent peut-être être séparés provoquée par d'autres entiers dans la permutation?

b) lorsqu'ils occupent des positions consécutives dans le tation?

30. Sept femmes et neuf hommes font partie du corps professoral département de mathématiques dans une école.

a) De combien de façons existe-t-il pour sélectionner un comité cinq membres du département si au moins une femme doit faire partie du comité?

b) De combien de façons existe-t-il pour sélectionner un comité cinq membres du département si au moins une femme et au moins un homme doit faire partie du comité?

31. L'alphabet anglais contient 21 consonnes et cinq les voyelles. Combien de chaînes de six lettres minuscules du L'alphabet anglais contient positions possibles pour les hommes.]

25. Cent billets, numérotés 1 , 2 , 3 , ..., 100, sont vendus à 100 personnes différentes pour un dessin. Quatre prix différents sont décernés, dont un grand prix (un voyage à Tahiti). Comment il existe de nombreuses façons d'attribuer les prix si

a) il n'y a pas de restrictions?
b) la personne qui détient le billet 47 remporte le grand prix?
c) la personne détenant le billet 47 remporte l'un des prix?
d) la personne qui détient le billet 47 ne gagne pas de prix?
e) les détenteurs des billets 19 et 47 gagnent-ils tous deux des prix?
f) les détenteurs des billets 19, 47 et 73 gagnent tous prix?
g) les détenteurs des billets 19, 47, 73 et 97 gagnent tous prix?
h) aucune des personnes détenant des billets 19, 47, 73 et 97 gagne un prix?
i) le gagnant du grand prix est une personne détenant un billet 19, 47, 73 ou 97?
j) les détenteurs des billets 19 et 47 gagnent des prix, mais les détenteurs de billets 73 et 97 ne gagnent pas de prix?

26. Treize personnes dans une équipe de softball se présentent pour un match.

a) Combien y a-t-il de façons de choisir 10 joueurs à prendre le champ?
b) De combien de façons existe-t-il pour attribuer les 10 postes en sélectionnant des joueurs parmi les 13 personnes qui se présentent?
c) Sur les 13 personnes qui se présentent, trois sont des femmes. Comment il existe de nombreuses façons de choisir 10 joueurs pour terrain si au moins un de ces joueurs doit être une femme?

27. Un club compte 25 membres.

a) De combien de façons existe-t-il pour choisir quatre membres le club pour faire partie d'un comité exécutif?
b) De combien de façons existe-t-il pour choisir un président, un vice président, secrétaire et trésorier du club, où personne ne peut occuper plus d'un poste?

a) exactement une voyelle?
b) exactement deux voyelles?
c) au moins une voyelle?
d) au moins deux voyelles?

32. Combien de chaînes de six lettres minuscules de l'En- alphabet glish contiennent

a) la lettre *a* ?
b) les lettres *a* et *b* ?
c) les lettres *a* et *b* dans des positions consécutives avec *un* *b* précédent , avec toutes les lettres distinctes?
d) les lettres *a* et *b* , où *a* est quelque part à gauche de *b* dans la chaîne, avec toutes les lettres distinctes?

33. Supposons qu'un département compte 10 hommes et 15 femmes. Combien de façons existe-t-il pour former un avec six membres s'il doit avoir le même nombre de hommes et femmes?

34. Supposons qu'un département compte 10 hommes et 15 femmes. Combien de façons existe-t-il pour former un avec six membres s'il doit y avoir plus de femmes que Hommes?

35. Combien de chaînes de bits contiennent exactement huit 0 et 10 1 si chaque 0 doit être immédiatement suivi d'un 1?

36. Combien de chaînes de bits contiennent exactement cinq 0 et 14 1 si chaque 0 doit être immédiatement suivi de deux 1?

37. Combien de chaînes de bits de longueur 10 contiennent au moins trois 1 et au moins trois 0?

38. De combien de manières existe-t-il pour sélectionner 12 pays Organisation des Nations Unies siégeant à un conseil si 3 sont sélectionnés parmi un bloc de 45, 4 sont sélectionnés dans un bloc de 57, et les autres sont sélectionnés parmi les 69 pays restants?

39. Combien de plaques d'immatriculation composées de trois lettres abaissé de trois chiffres ne contient aucune lettre ou chiffre deux fois?

Une ***r*** **- permutation circulaire de *n*** personnes est un siège de *r* de ces *n* personnes autour d'une table circulaire, où les sièges sont considérés comme identiques s'ils peuvent être obtenus les uns des autres en tournant la table.

40. Trouvez le nombre de 3 permutations circulaires de 5 personnes.

41. Trouver une formule pour le nombre de *r*- permutations circulaires de *n* personnes.

42. Trouver une formule pour le nombre de façons de placer *r* de *n* personnes autour d'une table circulaire, où les sièges sont considérés même si chaque personne a les mêmes deux voisins sans de quel côté ces voisins sont assis.

43. Combien de façons existe-t-il pour une course de chevaux avec trois des chevaux à finir si des attaches sont possibles? [*Remarque:* deux ou trois les chevaux peuvent attacher.]

∗ **44.** Combien de façons existe-t-il pour une course de chevaux avec quatre chevaux terminer si des liens sont possibles? [*Remarque:* N'importe quel nombre de quatre chevaux peuvent être à égalité.)

∗ **45.** Il y a six coureurs dans le tableau de bord des 100 verges. Combien il y a moyen de décerner trois médailles en cas d'égalité sont possibles? (Le ou les coureurs qui terminent avec le meilleur temps recevoir des médailles d'or, le ou les coureurs qui terminent avec exactement un coureur devant eux reçoivent de l'argent médailles, et le ou les coureurs qui terminent exactement deux coureurs devant reçoivent des médailles de bronze.)

∗ **46.** Cette procédure est utilisée pour rompre les égalités dans les matchs du championnat. tour pionnier du tournoi de football de la Coupe du monde. Chaque l'équipe sélectionne cinq joueurs dans un ordre prescrit. Chacun des ces joueurs prennent un coup de pied de pénalité, avec un joueur de la première équipe suivie d'un joueur de la deuxième équipe et ainsi de suite, en suivant l'ordre des joueurs spécifié. Si le score est toujours à égalité à la fin des 10 tirs au but, cette procédure la procédure est répétée. Si le score est toujours à égalité après 20 pénalités coups de pied, une fusillade de mort subite se produit, avec la première équipe marquer un but sans réponse victorieux.

a) Combien de scénarios de notation différents sont possibles si le match est réglé au premier tour de pénalité de 10 coups de pied, où le tour se termine une fois qu'il est impossible pour une équipe pour égaler le nombre de buts marqués par le autre équipe?
b) Combien de scénarios de notation différents pour le premier et deuxièmes groupes de tirs au but sont possibles si le jeu est réglé au deuxième tour de pénalité de 10 coups de pied?
c) Combien de scénarios de notation sont possibles pour ensemble de coups de pied de pénalité si le jeu est réglé sans plus de 10 coups de pied supplémentaires au total après les deux cinq coups de pied pour chaque équipe?

Coefficients et identités binomiaux

Comme nous l'avons remarqué à la section 6.3, le nombre decombinaisons *r* d'un ensemble avec *n* éléments est souvent désigné par $\binom{n}{r}$. Ce nombre est également appelé **coefficient binomial** car ces nombres se produisent sous forme de coefficients dans l'expansion des puissances d'expressions binomiales telles que $(a+b)^n$ nous discutera du **théorème binomial** , qui donne la puissance d'une expression binomiale comme une somme de termes impliquant des coefficients binomiaux. Nous prouverons ce théorème en utilisant une preuve combinatoire. Nous montrerons également comment les preuves combinatoires peuvent être utilisées pour établir certaines des nombreuses identités qui expriment des relations entre les coefficients binomiaux.

Le théorème binomial

Le théorème binomial donne les coefficients de l'expansion des puissances des expressions binomiales. Une expression **binomiale** est simplement la somme de deux termes, tels que $x + y$. (Les termes peuvent être des produits de constantes et de variables, mais cela ne nous concerne pas ici.)

L'exemple 1 illustre comment les coefficients d'une expansion typique peuvent être trouvés et prépare nous pour l'énoncé du théorème binomial.

EXEMPLE 1 L'expansion de $(x + y)^3$ peut être trouvée en utilisant le raisonnement combinatoire au lieu de multiplier les trois termes sur. Lorsque $(x + y)^3 = (x + y)(x + y)(x + y)$ est développé, tous les produits d'un terme dans la première somme, un terme dans la deuxième somme et un terme dans la troisième somme sont ajoutés. Conditions de les formes x^3, x^2y, xy^2 et y^3 apparaissent. Pour obtenir un terme de la forme x^3, un x doit être choisi dans chacune des sommes, et cela ne peut se faire que d'une seule façon. Ainsi, le terme x^3 dans le produit a un coefficient de 1. Pour obtenir un terme de la forme x^2y, un x doit être choisi dans deux des trois des sommes (et par conséquent un y dans l'autre somme). Par conséquent, le nombre de ces termes est le nombre de 2 combinaisons de trois objets, à savoir, $\binom{3}{2}$. De même, le nombre de termes du formulaire xy^2 est le nombre de façons de choisir l'une des trois sommes pour obtenir un x (et par conséquent prendre un y

de chacune des deux autres sommes). Cela peut être fait en $\binom{3}{1}$ façons. Enfin, le seul moyen d'obtenir un terme y^3 consiste à choisir le y pour chacune des trois sommes du produit, ce qui peut être fait en exactement dans un sens. Par conséquent, il s'ensuit que

$$\begin{aligned}(x + y)^3 &= (x + y)(x + y)(x + y) = (xx + xy + yx + yy)(x + y)\\ &= xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy\\ &= x^3 + 3x^2y + 3xy^2 + y^3.\end{aligned}$$

▲

Nous énonçons maintenant le théorème binomial.

THÉORÈME 1 **LE THÉORÈME BINOMIAL** Soit x et y *des* variables, et soit n un entier non négatif. alors

$$(x + y)^n = \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Preuve: Nous utilisons une preuve combinatoire. Les termes du produit lors de son expansion sont de la forme $x^{n-j}y^j$ pour $j = 0, 1, 2, \ldots, n$. Compter le nombre de termes de la forme $x^{n-j}y^j$, notons que pour obtenir un tel terme il faut choisir $n - j$ x s parmi les n sommes (pour que le les autres termes j du produit sont y s). Par conséquent, le coefficient de $x^{n-j}y^j$ est $\binom{n}{n-j}$, lequel est égal à $\binom{n}{j}$. Cela prouve le théorème.

Certaines utilisations informatiques du théorème binomial sont illustrées dans les exemples 2 à 4.

EXEMPLE 2 Quelle est l'expansion de $(x + y)^4$?

Solution: du théorème binomial, il s'ensuit que

$$\begin{aligned}(x + y)^4 &= \sum_{j=0}^{4}\binom{4}{j}x^{4-j}y^j\\ &= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4\\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.\end{aligned}$$

▲

EXEMPLE 3 Quel est le coefficient de $x^{12}y^{13}$ dans l'expansion de $(x + y)^{25}$?

Solution: du théorème binomial, il s'ensuit que ce coefficient est

$$\binom{25}{13} = \frac{25!}{13!\,12!} = 5,200,300.$$

▲

EXEMPLE 4 Quel est le coefficient de $x^{12}y^{13}$ dans l'expansion de $(2x - 3y)^{25}$?

Solution: Tout d'abord, notez que cette expression est égale à $(2x + (-3y))^{25}$. Par le théorème binomial, nous avoir

$$(2x+(-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j .$$

Par conséquent, le coefficient de $x^{12} y^{13}$ dans l'expansion est obtenu lorsque $j = 13$, à savoir,

$$\binom{25}{13} 2^{12} (-3)^{13} = -\frac{25!}{13!\,12!} 2^{12} 3^{13} .$$

▲

Nous pouvons prouver quelques identités utiles en utilisant le théorème binomial, comme les corollaires 1, 2 et 3 démontrer.

COROLLARY 1 Soit n un entier non négatif. alors

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n .$$

Preuve: En utilisant le théorème binomial avec $x = 1$ et $y = 1$, nous voyons que

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} .$$

C'est le résultat souhaité.

Il y a aussi une belle preuve combinatoire du Corollaire 1, que nous présentons maintenant.

Preuve: un ensemble avec n éléments a un total de 2^n sous-ensembles différents. Chaque sous-ensemble n'a aucun élément, un élément, deux éléments, ..., ou n éléments en elle. Il y a $\binom{n}{0}$ des sous-ensembles à zéro élément, $\binom{n}{1}$ sous-ensembles avec un élément, $\binom{n}{2}$ sous-ensembles à deux éléments, ..., et $\binom{n}{n}$ sous-ensembles avec n éléments. Donc,

$$\sum_{k=0}^{n} \binom{n}{k}$$

compte le nombre total de sous-ensembles d'un ensemble avec n éléments. En assimilant les deux formules, nous avoir pour le nombre de sous-ensembles d'un ensemble avec n éléments, nous voyons que

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n .$$

COROLLARY 2 Soit n un entier positif. alors

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 .$$

Preuve: lorsque nous utilisons le théorème binomial avec $x = -1$ et $y = 1$, nous voyons que

$$0 = 0^n = ((-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k .$$

Cela prouve le corollaire.

Remarque: le corollaire 2 implique que

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=\binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots.$$

COROLLARY 3 Soit n un entier non négatif. alors

$$\sum_{k=0}^{n} 2^k\binom{n}{k}=3^n.$$

Preuve: Nous reconnaissons que le côté gauche de cette formule est l'expansion de $(1+2)^n$ à condition de par le théorème binomial. Par conséquent, par le théorème binomial, nous voyons que

$$(1+2)^n=\sum_{k=0}^{n}\binom{n}{k}1^{n-k}2^k=\sum_{k=0}^{n}\binom{n}{k}2^k.$$

Par conséquent

$$\sum_{k=0}^{n} 2^k\binom{n}{k}=3^n.$$

Identité et triangle de Pascal

Les coefficients binomiaux satisfont de nombreuses identités différentes. Nous introduisons l'un des plus important de ces maintenant.

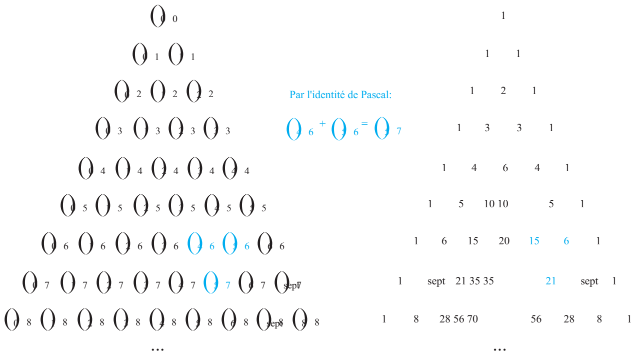
THÉORÈME 2 **IDENTITÉ DE PASCAL** Soit n et k des entiers positifs avec $n \geq k$. alors

$$\binom{n+1}{k}=\binom{n}{k-1}+\binom{n}{k}.$$

Preuve: Nous utiliserons une preuve combinatoire. Supposons que T soit un ensemble contenant $n+1$ éléments. Laisser a être un élément dans T, et soit $S=T-\{a\}$. Notez qu'il existe $\binom{n+1}{k}$ sous-ensembles de T contenant k éléments. Cependant, un sous-ensemble de T avec k éléments contient soit *un* ensemble avec $k-1$ éléments de S, ou contient k éléments de S et ne contient pas a. Parce qu'il y a $\binom{n}{k-1}$ sous-ensembles de $k-1$ éléments de S, il y a $\binom{n}{k-1}$ sous-ensembles de k éléments de T qui contiennent a. Et il y a $\binom{n}{k}$ sous-ensembles de k éléments de T qui ne contiennent pas a, car il y a $\binom{n}{k}$ sous-ensembles de k éléments de S. Par conséquent,

$$\binom{n+1}{k}=\binom{n}{k-1}+\binom{n}{k}.$$

Remarque: Il est également possible de prouver cette identité par manipulation algébrique à partir de la formule pour $\binom{n}{r}$ (voir exercice 19).



(une) b)

FIGURE 1 **Triangle de Pascal.**

Remarque: l'identité de Pascal, ainsi que les conditions initiales $\binom{n}{0} = \binom{n}{n} = 1$ pour tous les entiers n , peut être utilisé pour définir récursivement des coefficients binomiaux. Cette définition récursive est utile dans le calcul des coefficients binomiaux car seule l'addition, et non la multiplication, des entiers est nécessaire pour utiliser cette définition récursive.

L'identité de Pascal est la base d'un arrangement géométrique des coefficients binomiaux dans un triangle, comme le montre la figure 1.

La n ème ligne du triangle est constituée des coefficients binomiaux

$$\binom{n}{k}, \ k = 0, 1, \ldots, n.$$

Ce triangle est connu sous le nom **de triangle de Pascal** . L'identité de Pascal montre que lorsque deux les coefficients binomiaux dans ce triangle sont ajoutés, le coefficient binomial dans la ligne suivante entre ces deux coefficients sont produits.

BLAISE PASCAL (1623-1662) Blaise Pascal a montré ses talents à un âge précoce, bien que son père, qui avait fait des découvertes en géométrie analytique, gardé des livres de mathématiques loin de lui pour encourager d'autres intérêts. A 16 ans, Pascal découvre un résultat important concernant les sections coniques. À 18 ans, il a conçu une machine à calculer, qu'il a construit et vendu. Pascal et Fermat ont jeté les bases de la théorie moderne des probabilités. Dans ce travail, il a fait de nouvelles découvertes concernant ce qu'on appelle aujourd'hui le triangle de Pascal. En 1654, Pascal abandonne ses recherches mathématiques pour se consacrer à la théologie. Après cela, il n'est retourné aux mathématiques qu'une seule fois. Un la nuit, distrait par un mal de dents sévère, il chercha du réconfort en étudiant les propriétés mathématiques de la cycloïde. Miraculeusement, sa douleur s'est apaisée, ce qu'il a considéré comme un signe d'approbation divine de l'étude des mathématiques.

Autres identités impliquant des coefficients binomiaux

Nous concluons cette section avec des preuves combinatoires de deux des nombreuses identités dont jouit les coefficients binomiaux.

THÉORÈME 3 **IDENTITÉ DE VANDERMONDE** Soit m, n et r des entiers non négatifs avec r non dépassant m ou n. alors

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}.$$

Remarque: cette identité a été découverte par le mathématicien Alexandre-Théophile Vandermonde au XVIIIe siècle.

Preuve: Supposons qu'il y ait m éléments dans un ensemble et n éléments dans un second ensemble. Ensuite, le total nombre de façons de choisir r éléments de l'union de ces ensembles est $\binom{m+n}{r}$.

Une autre façon de choisir r éléments de l'union est de choisir k éléments du deuxième ensemble puis $r-k$ éléments du premier ensemble, où k est un entier avec $0 \le k \le r$. Parce que là sont $\binom{n}{k}$ façons de choisir k éléments du deuxième ensemble et $\binom{m}{r-k}$ façons de choisir les éléments $r-k$ à partir du premier ensemble, la règle du produit nous dit que cela peut être fait en $\binom{m}{r-k}\binom{n}{k}$ façons. D'où le le nombre total de façons de choisir r éléments de l'union est également égal à $\sum_{k=0}^{r}\binom{m}{r-k}\binom{n}{k}$.

Nous avons trouvé deux expressions pour le nombre de façons de choisir r éléments du union d'un ensemble avec m éléments et d'un ensemble avec n éléments. Leur égalisation nous donne la identité.

Le corollaire 4 découle de l'identité de Vandermonde.

COROLLARY 4 Si n est un entier non négatif, alors

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

Preuve: on utilise l'identité de Vandermonde avec $m = r = n$ pour obtenir

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{n-k}\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

La dernière égalité a été obtenue en utilisant l'identité $\binom{n}{k} = \binom{n}{n-k}$.

ALEXANDRE-THÉOPHILE VANDERMONDE (1735–1796) Parce qu'Alexandre-Théophile Vandermonde était un enfant maladif, son père médecin lui a orienté vers une carrière musicale. Cependant, il a développé plus tard un intérêt pour les mathématiques. Son mathématique complète le travail consiste en quatre articles publiés en 1771–1772. Ces articles comprennent des contributions fondamentales sur les racines des équations, sur la théorie des déterminants et le problème du tour du chevalier (introduit dans les exercices de la section 10.5). L'intérêt de Vandermonde pour les mathématiques n'ont duré que 2 ans. Par la suite, il a publié des articles sur l'harmonie, les expériences avec le froid et la fabrication de l'acier. Il s'est également intéressé à la politique, rejoignant la cause de la révolution française et occupant plusieurs postes différents au sein du gouvernement.

Nous pouvons prouver les identités combinatoires en comptant les chaînes de bits avec différentes propriétés, comme la preuve du Théorème 4 le démontrera.

THÉORÈME 4 Soit n et r des entiers non négatifs avec $r \le n$. alors

$$(\quad) \quad \sum^{n} (\quad)$$

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}.$$

Preuve: Nous utilisons une preuve combinatoire. Par l'exemple 14 de la section 6.3, le côté gauche, $\binom{n+1}{r+1}$, compte les chaînes de bits de longueur $n + 1$ contenant $r + 1$ unités.

Nous montrons que le côté droit compte les mêmes objets en considérant les cas corres- répondre aux emplacements possibles du 1 final dans une chaîne avec $r + 1$ unités. Ce dernier doit se produire à la position $r + 1, r + 2, \ldots$ ou $n + 1$. De plus, si le dernier est le k ème bit, il doit être r parmi les k -1 premières positions. Par conséquent, par l'exemple 14 de la section 6.3, sont $\binom{k-1}{r}$ ces chaînes de bits. En sommant k avec $r + 1 \leq k \leq n + 1$, on trouve qu'il y a

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r} = \sum_{j=r}^{n} \binom{j}{r}$$

chaînes de bits de longueur n contenant exactement $r + 1$ unités. (Notez que la dernière étape découle de la changement de variables $j = k - 1$.) Parce que le côté gauche et le côté droit comptent le mêmes objets, ils sont égaux. Ceci complète la preuve.

Des exercices

1. Trouvez l'expansion de $(x + y)^4$

a) en utilisant le raisonnement combinatoire, comme dans l'exemple 1.
b) en utilisant le théorème binomial.

2. Trouvez l'expansion de $(x + y)^5$

a) en utilisant le raisonnement combinatoire, comme dans l'exemple 1.
b) en utilisant le théorème binomial.

3. Trouvez l'expansion de $(x + y)^6$.

4. Trouvez le coefficient de x^5y^8 in $(x + y)^{13}$.

5. Combien de termes y a-t-il dans l'expansion de $(x + y)^{100}$ après que des termes similaires soient collectés?

6. Quel est le coefficient de x^7 dans $(1 + x)^{11}$?

7. Quel est le coefficient de x^9 dans $(2 - x)^{19}$?

8. Quel est le coefficient de x^8y^9 dans l'expansion de $(3x + 2$ ans $)^{17}$?

9. Quel est le coefficient de $x^{101}y^{99}$ dans l'expansion de $(2x - 3$ ans $)^{200}$?

∗ **10.** Donner une formule pour le coefficient de x^k dans l'expansion de $(x + 1/x)^{100}$, où k est un entier.

∗ **11.** Donner une formule pour le coefficient de x^k dans l'expansion de $(x^2 - 1/x)^{100}$, où k est un entier.

12. La rangée du triangle de Pascal contenant le co- binôme binomial efficients $\binom{10}{k}$, $0 \leq k \leq 10$, est:

1 10 45 120 210 252 210 120 45 10 1

Utilisez l'identité de Pascal pour produire la ligne immédiatement après en descendant cette ligne dans le triangle de Pascal.

13. Quelle est la rangée du triangle de Pascal contenant le bino- coefficients miaux $\binom{9}{k}$, $0 \leq k \leq 9$?

14. Montrer que si n est un entier positif, alors $1 = \binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil} > \cdots > \binom{n}{n-1} > \binom{n}{n} = 1$.

15. Montrez que $\binom{n}{k} \leq 2^n$ pour tous les entiers positifs n et tous les tegers k avec $0 \leq k \leq n$.

16. a) Utilisez l'exercice 14 et le corollaire 1 pour montrer que si n est un entier supérieur à 1, puis $\binom{n}{\lfloor n/2\rfloor} \geq 2^n/n$.

b) conclure de la partie (a) que si n est un entier positif, ensuite $\binom{2n}{n} \geq 4^n/2n$.

17. Montrer que si n et k sont des entiers avec $1 \leq k \leq n$, alors $\binom{n}{k} \leq n^k/2^{k-1}$.

18. Supposons que b soit un entier avec $b \geq 7$. Utilisez le bino- théorème mial et la ligne appropriée du triangle de Pascal pour trouver l' expansion de base- b de $(11_b)^4$ [c'est-à-dire le quatrième puissance du nombre $(11)_b$ en notation base- b].

19. Prouver l'identité de Pascal, en utilisant la formule pour $\binom{n}{r}$.

20. Supposons que k et n sont des entiers avec $1 \leq k < n$. Prouver l' **identité hexagonale**

$$\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} = \binom{n-1}{k}\binom{n}{k-1}\binom{n+1}{k+1},$$

qui relie les termes du triangle de Pascal qui forment un hexagone.

21. Démontrer que si n et k sont des entiers avec $1 \leq k \leq n$, alors $k\binom{n}{k} = n\binom{n-1}{k-1}$,

a) en utilisant une preuve combinatoire. [*Indice:* montrez que les deux côtés de l'identité comptent le nombre de façons de sélectionner un sous-ensemble avec k éléments d'un ensemble avec n éléments puis un élément de ce sous-ensemble.]

b) en utilisant une preuve algébrique basée sur la formule pour $\binom{n}{r}$ donnée dans le théorème 2 de la section 6.3.

22. Prouver l'identité $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$, chaque fois que n, r et k sont des entiers non négatifs avec $r \leq n$ et $k \leq r$,

a) en utilisant un argument combinatoire.

b) en utilisant un argument basé sur la formule du nombre ber de r -combinaisons d'un ensemble avec n éléments.

23. Montrer que si n et k sont des entiers positifs, alors

$$\binom{n+1}{k} = (n+1)\binom{n}{k-1}\Big/k.$$

Utilisez cette identité pour construire une définition inductive de les coefficients binomiaux.

24. Montrer que si p est un nombre premier et k est un entier tel que $1 \leq k \leq p - 1$, alors p divise $\binom{p}{k}$.

33. Dans cet exercice, nous allons compter le nombre de chemins dans le plan xy entre l'origine (0, 0) et le point (m, n), où m et n sont des entiers non négatifs, tels que chaque chemin est composé d'une série d'étapes, où chaque étape est un mouvement l'unité vers la droite ou déplacer une unité vers le haut. (Aucun mouvement vers gauche ou vers le bas sont autorisés.) Deux de ces chemins de $(0, 0)$ à $(5, 3)$ sont illustrés ici.

(5, 3)

(0, 0)

(5, 3)

25. Soit n un entier positif. Montre CA

$$\binom{2n}{n+1} + \binom{2n}{n} = \binom{2n+2}{n+1} / 2 .$$

$*$ **26.** Soit n et k *des* entiers avec $1 \leq k \leq n$. Montre CA

$$\sum_{k=1}^{n} \binom{n}{k}\binom{n}{k-1} = \binom{2n+2}{n+1} / 2 - \binom{2n}{n} .$$

$*$ **27.** Prouver l' **identité de** la **cloche**

$$\sum_{k=0}^{r} \binom{n+k}{k} = \binom{n+r+1}{r}$$

chaque fois que n et r sont des entiers positifs,

a) en utilisant un argument combinatoire.

b) utiliser l'identité de Pascal.

28. Montrer que si n est un entier positif, alors $\binom{2n}{2} = 2\binom{n}{2} + n^2$

a) en utilisant un argument combinatoire.

b) par manipulation algébrique.

$*$ **29.** Donnez une preuve combinatoire que $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.

[*Astuce:* comptez de deux façons le nombre de façons de sélectionner et de sélectionner ensuite un chef de file du comité.]

$*$ **30.** Donnez une preuve combinatoire que $\sum_{k=1}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}$.

[*Astuce:* comptez de deux façons le nombre de façons de sélectionner comité, avec n membres d'un groupe de n mathé- professeurs d'ICS et n professeurs d'informatique, que le président du comité est un mathématique professeur.]

31. Montrer qu'un ensemble non vide a le même nombre de sous-ensembles avec un nombre impair d'éléments comme il le fait avec des sous-ensembles un nombre pair d'éléments.

$*$ **32.** Démontrer le théorème binomial à l'aide d'inductions mathématiques

tion.

(0, 0)

a) Montrer que chaque chemin du type décrit peut être représenté ressenti par une chaîne de bits composée de m 0s et n 1s, où un 0 représente un déplacement d'une unité vers la droite et un 1 représente un déplacement d'une unité vers le haut.

b) conclure de la partie a) qu'il y a $\binom{m+n}{n}$ chemins de le type souhaité.

34. Utilisez l'exercice 33 pour donner une autre preuve du corollaire 2 à la section 6.3, qui stipule que $\binom{n}{k} = \binom{n}{n-k}$ chaque fois que k est un entier avec $0 \leq k \leq n$. [*Indice:* considérez le nombre des chemins du type décrit dans l'exercice 33 à partir de $(0, 0)$ à $(n-k, k)$ et de $(0, 0)$ à $(k, n-k)$.]

35. Utilisez l'exercice 33 pour prouver le théorème 4. [*Indice:* comptez le nombre de chemins avec n étapes du type décrit dans exercice 33. Chaque chemin doit se terminer à l'un des points $(n-k, k)$ pour $k = 0, 1, 2, \ldots, n$.]

36. Utilisez l'exercice 33 pour prouver l'identité de Pascal. [*Astuce:* Afficher qu'un chemin du type décrit dans l'exercice 33 de $(0, 0)$ à $(n+1-k, k)$ passe soit par $(n+1-k, k-1)$ ou $(n-k, k)$, mais pas par les deux.]

37. Utilisez l'exercice 33 pour prouver l'identité du jarret Exercice 27. [*Astuce:* Tout d'abord, notez que le nombre de les chemins de $(0, 0)$ à $(n+1, r)$ *sont* égaux $\binom{n+1+r}{r}$. Seconde- deuxièmement, compter le nombre de chemins en additionnant le nombre ber de ces chemins qui commencent par aller k unités vers le haut pour $k = 0, 1, 2, \ldots, r$.]

38. Donner une preuve combinatoire que si n est un entier positif ger alors $\sum_{k=0}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2}$. [*Indice:* montrez que les deux côtés comptent les façons de sélectionner un sous-ensemble d'un ensemble de n éléments avec deux éléments pas nécessairement distincts de ce sous-ensemble. En outre, exprimez le côté droit comme $n(n-1)2^{n-2} + n2^{n-1}$.]

$*$ **39.** Déterminer une formule impliquant des coefficients binomiaux pour le n ème terme d'une séquence si ses termes initiaux sont ceux répertoriés. [*Astuce:* Regarder le triangle de Pascal sera utile.

Bien qu'une infinité de séquences commencent par un nombre spécifié ensemble de termes, chacune des listes suivantes est le début d'un séquence du type souhaité.]

a) 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66 , ...

b) 1, 4, 10, 20, 35, 56, 84, 120, 165, 220 , ...

c) 1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620 , ...

d) 1, 1, 2, 3, 6, 10, 20, 35, 70, 126 , ...

e) 1, 1, 1, 3, 1, 5, 15, 35, 1, 9 , ...

f) 1, 3, 15, 84, 495, 3003, 18564, 116280, 735471, 4686825 , ...

Permutations et combinaisons généralisées

introduction

Dans de nombreux problèmes de comptage, les éléments peuvent être utilisés à plusieurs reprises.Par exemple, une lettre ou un chiffre peut être utilisé plus d'une fois sur une plaque d'immatriculation. Lorsqu'une douzaine de beignets sont sélectionnés, chaque variété peut être choisi à plusieurs reprises. Cela contraste avec les problèmes de comptage abordés plus haut dans le chapitre où nous avons considéré uniquement les permutations et les combinaisons dans lesquelles chaque élément pouvait être utilisé à la plupart du temps. Dans cette section, nous allons montrer comment résoudre les problèmes de comptage où les éléments peuvent être utilisé plus d'une fois.

De plus, certains problèmes de comptage impliquent des éléments indiscernables.Par exemple, pour compter nombre de façons dont les lettres du mot *SUCCÈS* peuvent être réorganisées, le placement de les lettres doivent être prises en considération.Cela contraste avec les problèmes de comptage évoqués plus haut, où tous les les éléments ont été considérés comme distinguables. Dans cette section, nous décrirons comment résoudre le comptage problèmes dans lesquels certains éléments sont indiscernables.

De plus, dans cette section, nous expliquerons comment résoudre une autre classe importante de comptage problèmes, problèmes liés au comptage des façons de placer des éléments des boites. Un exemple de ce type de problème est le nombre de façons dont les mains de poker peuvent être distribué à quatre joueurs.

Ensemble, les méthodes décrites précédemment dans ce chapitre et les méthodes introduites dans cette section forme une boîte à outils utile pour résoudre un large éventail de problèmes de comptage.Quand le des méthodes supplémentaires discutées au chapitre 8 sont ajoutées à cet arsenal, vous pourrez résoudre un pourcentage élevé des problèmes de comptage qui se posent dans un large éventail de domaines d'études.

Permutations avec répétition

Le comptage des permutations lorsque la répétition des éléments est autorisée peut facilement être effectué à l'aide du règle du produit, comme le montre l'exemple 1.

EXEMPLE 1 Combien de chaînes de longueur r peuvent être formées à partir des lettres majuscules de l'alphabet anglais?

Solution: selon la règle du produit, car il y a 26 lettres anglaises majuscules et parce que chaque lettre peut être utilisée à plusieurs reprises, nous voyons qu'il y a 26^r chaînes de lettres anglaises majuscules de longueur r . ▲

Le nombre de r- permutations d'un ensemble avec n éléments lorsque la répétition est autorisée est donné dans le théorème 1.

THÉORÈME 1 Le nombre de r- permutations d'un ensemble de n objets avec répétition autorisée est n^r .

Preuve: Il y a n façons de sélectionner un élément de l'ensemble pour chacune des r positions dans le r- permutation lorsque la répétition est autorisée, car pour chaque choix tous les n objets sont disponibles.
Par conséquent, la règle du produit il y a n^r r -permutations lorsque la répétition est autorisée.

Combinaisons avec répétition

Considérez ces exemples de combinaisons avec répétition d'éléments autorisés.

EXEMPLE 2 De combien de façons existe-t-il pour sélectionner quatre fruits dans un bol contenant des pommes, des oranges, et les poires si l'ordre dans lequel les morceaux sont sélectionnés n'a pas d'importance, seul le type de fruit et pas le morceau individuel importe, et il y a au moins quatre morceaux de chaque type de fruit dans le bol?

Solution: Pour résoudre ce problème, nous énumérons toutes les façons possibles de sélectionner le fruit. Il y a 15 façons:

4 pommes	4 oranges	4 poires
3 pommes, 1 orange	3 pommes, 1 poire	3 oranges, 1 pomme
3 oranges, 1 poire	3 poires, 1 pomme	3 poires, 1 orange
2 pommes, 2 oranges	2 pommes, 2 poires	2 oranges, 2 poires
2 pommes, 1 orange, 1 poire	2 oranges, 1 pomme, 1 poire	2 poires, 1 pomme, 1 orange

La solution est le nombre de 4 combinaisons avec répétition autorisées à partir d'un ensemble à trois éléments, { *pomme* , *orange* , *poire* }. ▲

Pour résoudre des problèmes de comptage plus complexes de ce type, nous avons besoin d'une méthode générale compter les combinaisons r d'un ensemble d'éléments n . Dans l'exemple 3, nous illustrerons une telle méthode.

EXEMPLE 3 De combien de façons existe-t-il pour sélectionner cinq billets dans une caisse contenant des billets de 1 $, 2 $, 5 $ factures, 10 $, 20 $, 50 $ et 100 $? Supposons que l'ordre dans lequel les factures sont choisi n'importe pas, que les factures de chaque dénomination soient indiscernables et qu'il sont au moins cinq factures de chaque type.

Solution: Parce que l'ordre dans lequel les factures sont sélectionnées n'a pas d'importance et sept différents types de factures peuvent être sélectionnés jusqu'à cinq fois, ce problème implique le comptage 5 combinaisons avec répétition autorisées à partir d'un ensemble de sept éléments. Liste de toutes les possibilités serait fastidieux, car il existe un grand nombre de solutions. Au lieu de cela, nous illustrerons la utilisation d'une technique de comptage des combinaisons avec répétition autorisée.

Supposons qu'une caisse à billets comporte sept compartiments, un pour contenir chaque type de billet, comme illustré dans la figure 1. Ces compartiments sont séparés par six séparateurs, comme indiqué sur l'image. le le choix de cinq billets correspond à placer cinq marqueurs dans les compartiments contenant différents types de factures. La figure 2 illustre cette correspondance pour trois façons différentes de sélectionner cinq factures, où les six séparateurs sont représentés par des barres et les cinq billets par des étoiles.

Le nombre de façons de sélectionner cinq factures correspond au nombre de façons d'organiser six bars et cinq étoiles d'affilée avec un total de 11 positions. Par conséquent, le nombre de façons de sélectionner les cinq billets est le nombre de façons de sélectionner les positions des cinq étoiles parmi les 11 postes. Cela correspond au nombre de sélections non ordonnées de 5 objets parmi un ensemble de 11

100 $ 50 $ 20 $ 10 $ 5 $ 2 $ 1 $

FIGURE 1 **Caisse avec sept types de factures.**

dix 1
10$$ 10$$ ** ***
$ 10$
$

100 50 20 5
$$ $$ 10$$ $$ * * * * *
$

100 dix 2 1
$$ 10$$ $$ $$ * * * * *
$

FIGURE 2 **Exemples de façons de sélectionner cinq factures.**

objets, ce qui peut être fait de manière $C(11, 5)$. Par conséquent, il existe

$$C(11, 5) = \frac{11!}{5!\,6!} = 462$$

façons de choisir cinq billets dans la caisse avec sept types de billets. ▲

Le théorème 2 généralise cette discussion.

THÉORÈME 2 Il y a $C(n + r - 1, r) = C(n + r - 1, n - 1)$ r-combinaisons d'un ensemble avec n éléments lorsque la répétition des éléments est autorisée.

Preuve: chaque r-combinaison d'un ensemble avec n éléments lorsque la répétition est autorisée peut être ressenti par une liste de $n - 1$ barres et r étoiles. Les $n - 1$ barres sont utilisées pour marquer n différents cellules, avec la i ème cellule contenant une étoile pour chaque fois que le i ème élément de l'ensemble se produit dans le combinaison. Par exemple, une combinaison de 6 d'un ensemble de quatre éléments est représentée avec trois bars et six étoiles. Ici

** | * || ***

représente la combinaison contenant exactement deux du premier élément, l'un du deuxième élément, aucun du troisième élément, et trois du quatrième élément de l'ensemble.

Comme nous l'avons vu, chaque liste différente contenant $n - 1$ barres et r étoiles correspond à un r-combinaison de l'ensemble avec n éléments, lorsque la répétition est autorisée.Le nombre de ces listes est $C(n - 1 + r, r)$, car chaque liste correspond à un choix des r positions pour placer le r étoiles des positions $n - 1 + r$ qui contiennent r étoiles et $n - 1$ barres. Le nombre de ces listes est également égal à $C(n - 1 + r, n - 1)$, car chaque liste correspond à un choix des $n - 1$ positions pour placer les $n - 1$ barres.

Les exemples 4 à 6 montrent comment le théorème 2 est appliqué.

EXEMPLE 4 Supposons qu'une boutique de cookies possède quatre types de cookies différents.Combien de façons différentes peuvent choisir six cookies? Supposons que seul le type de cookie, et non les cookies individuels ou l'ordre dans lequel ils sont choisis importe.

Solution: Le nombre de façons de choisir six cookies est le nombre de 6 combinaisons d'un ensemble avec quatre éléments. D'après le théorème 2, cela équivaut à $C(4+6-1, 6) = C(9, 6)$. Car

$$C(9, 6) = C(9, 3) = \frac{9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3} = 84,$$

il y a 84 façons différentes de choisir les six cookies. ▲

Le théorème 2 peut également être utilisé pour trouver le nombre de solutions de certaines équations linéaires où les variables sont des entiers soumis à des contraintes.Ceci est illustré par l'exemple 5.

EXEMPLE 5 Combien de solutions l'équation

$$x_1 + x_2 + x_3 = 11$$

ont, où x_1, x_2 et x_3 sont des entiers non négatifs?

Solution: Pour compter le nombre de solutions, on note qu'une solution correspond à un moyen de sélection de 11 éléments dans un ensemble de trois éléments de sorte que x_1 éléments de type un, x_2 éléments de type deux et x_3 éléments de type trois sont choisis.Par conséquent, le nombre de solutions est égal au nombre de 11 combinaisons avec répétition autorisées à partir d'un ensemble à trois éléments.Du Théorème 2, il s'ensuit qu'il y a

$$C(3+11-1, 11) = C(13, 11) = C(13, 2) = \frac{13 \cdot 12}{1 \cdot 2} = 78$$

solutions.

Le nombre de solutions de cette équation peut également être trouvé lorsque les variables sont soumises aux contraintes. Par exemple, nous pouvons trouver le nombre de solutions où les variables sont intégrées gers avec $x_1 \geq 1$, $x_2 \geq 2$ et $x_3 \geq 3$. Une solution de l'équation soumise à ces contraintes correspond à une sélection de 11 éléments avec x_1 éléments de type un, x_2 éléments de type deux et x_3 éléments de type trois, où, en outre, il existe au moins un élément de type un, deux éléments de type deux et trois éléments de type trois.Ainsi, une solution correspond au choix d'un élément de type un, deux de type deux et trois de type trois, ainsi qu'un choix de cinq éléments supplémentaires de n'importe quel type. Selon le théorème 2, cela peut être fait en

$$C(3+5-1, 5) = C(7, 5) = C(7, 2) = \frac{7 \cdot 6}{1 \cdot 2} = 21$$

façons. Ainsi, il existe 21 solutions de l'équation soumises aux contraintes données. ▲

L'exemple 6 montre comment compter le nombre de combinaisons avec répétition autorisée se produit pour déterminer la valeur d'une variable qui est incrémentée à chaque fois qu'un certain type de boucle imbriquée est traversé.

TABLEAU 1 Combinaisons et permutations avec et sans répétition.

Type	*Répétition autorisée?*	*Formule*
r- permutations	Non	$\frac{n!}{(n-r)!}$
r -combinaisons	Non	$\frac{n!}{r!\,(n-r)!}$
r- permutations	Oui	n^r
r -combinaisons	Oui	$\frac{(n+r-1)!}{r!\,(n-1)!}$

EXEMPLE 6 Quelle est la valeur de k après l'exécution du pseudocode suivant?

```
k := 0
pour i1 := 1 à n
    pour i2 := 1 à i1
        .
        .
        .
        pour im := 1 à im-1
            k := k + 1
```

Solution: Notez que la valeur initiale de k est 0 et que 1 est ajouté à k chaque fois que la boucle imbriquée est parcouru avec une séquence d'entiers $i_1, i_2, \ldots, i_m$ tels que

$$1 \leq i_m \leq i_{m-1} \leq \cdots \leq i_1 \leq n.$$

Le nombre de telles séquences d'entiers est le nombre de façons de choisir m entiers parmi $\{1, 2, \ldots, n\}$, avec répétition autorisée. (Pour voir cela, notez qu'une fois qu'une telle séquence a été sélectionné, si nous ordonnons les nombres entiers dans la séquence dans un ordre non décroissant, cela définit uniquement une affectation de $i_m, i_{m-1}, \ldots, i_1$. Inversement, chaque mission de ce type correspond à un ensemble non ordonné.) Par conséquent, d'après le théorème 2, il s'ensuit que $k = C(n+m-1, m)$ après ce code a été exécuté. ▲

Les formules pour le nombre de sélections ordonnées et non ordonnées d'éléments r, choisies avec et sans répétition autorisés à partir d'un ensemble de n éléments, sont présentés dans le tableau 1.

Permutations avec des objets indiscernables

Certains éléments peuvent être impossibles à distinguer dans les problèmes de comptage. Dans ce cas, il faut être pris pour éviter de compter les choses plus d'une fois. Prenons l'exemple 7.

EXEMPLE 7 Combien de chaînes différentes peut-on faire en réordonnant les lettres du mot *SUCCESS* ?

Solution: Étant donné que certaines lettres de *SUCCÈS* sont identiques, la réponse n'est *pas* donnée par le nombre de permutations de sept lettres. Ce mot contient trois S s, deux C s, un U, et une E.
Pour déterminer le nombre de chaînes différentes pouvant être créées en réorganisant les lettres, notez d'abord que les trois S peuvent être placés parmi les sept positions de $C(7, 3)$ manières différentes, laissant quatre

postes libres. Ensuite, les deux C peuvent être placés de façon $C(4, 2)$, laissant deux positions libres. Le U peut être placé de la manière $C(2, 1)$, ne laissant qu'une seule position libre. Par conséquent, E peut être placé dans $C(1, 1)$ façon. Par conséquent, à partir de la règle du produit, le nombre de chaînes différentes qui peuvent être faites est

$$\begin{aligned} C(7,3)\,C(4,2)\,C(2,1)\,C(1,1) &= \frac{\text{sept!}}{3!\,4!}\cdot\frac{4!}{2!\,2!}\cdot\frac{2!}{1!\,1!}\cdot\frac{1!}{1!\,0!} \\ &= \frac{\text{sept!}}{3!\,2!\,1!\,1!} \\ &= 420. \end{aligned}$$

▲

Nous pouvons prouver le théorème 3 en utilisant le même type de raisonnement que dans l'exemple 7.

THÉORÈME 3 Le nombre de permutations différentes de n objets, où il y a n_1 indiscernable objets de type 1, n_2 objets indiscernables de type 2, ..., et n_k objets indiscernables de type k, est

$$\frac{n!}{n_1!\,n_2!\cdots n_k!}.$$

Preuve: Pour déterminer le nombre de permutations, notons d'abord que les n_1 objets de type un peuvent être placé parmi les n positions de façon $C(n, n_1)$, laissant $n - n_1$ positions libres. Ensuite, les objets de type deux peuvent être placés en $C(n - n_1, n_2)$, laissant $n - n_1 - n_2$ positions libres. Continuer placer les objets de type trois, ..., de type $k - 1$, jusqu'à la dernière étape, n_k objets de type k peut être placé de la manière $C(n - n_1 - n_2 - \cdots - n_{k-1}, n_k)$. Par conséquent, selon la règle du produit, le total nombre de permutations différentes est

$$\begin{aligned} &C(n, n_1)\,C(n - n_1, n_2)\cdots C(n - n_1 - \cdots - n_{k-1}, n_k) \\ &= \frac{n!}{n_1!\,(n-n_1)!}\,\frac{(n-n_1)!}{n_2!\,(n-n_1-n_2)!}\cdots\frac{(n-n_1-\cdots-n_{k-1})!}{n_k!\,0!} \\ &= \frac{n!}{n_1!\,n_2!\cdots n_k!}. \end{aligned}$$

Distribution d'objets dans des boîtes

De nombreux problèmes de comptage peuvent être résolus en énumérant les façons dont les objets peuvent être placés dans des boîtes (où l'ordre dans lequel ces objets sont placés dans les boîtes n'a pas d'importance). Les objets peuvent être soit *distinctes*, c'est-à-dire différentes les unes des autres, soit *indiscernables*, c'est-à-dire considérées identique. On dit parfois que les objets distinctifs sont *étiquetés*, alors que les objets ne seraient pas *étiquetés*. De même, les boîtes peuvent être *distinguées*, c'est-à-dire différentes, ou *indiscernables*, c'est-à-dire identiques. On dit souvent que les boîtes distinctes sont *étiquetées*, les boîtes indiscernables ne seraient pas *étiquetées*. Lorsque vous résolvez un problème de comptage à l'aide de le modèle de distribution des objets dans des boîtes, vous devez déterminer si les objets sont distinctes et si les boîtes sont distinctes. Bien que le contexte du comptage problème rend ces deux décisions claires, les problèmes de comptage sont parfois ambigus et il peut ne pas être clair quel modèle s'applique. Dans un tel cas, il est préférable de formuler toutes les hypothèses que vous faites et expliquez pourquoi le modèle particulier que vous choisissez est conforme à vos hypothèses.

Nous verrons qu'il existe des formules fermées pour compter les façons de distribuer les objets, distinguable ou indiscernable, dans des boîtes distinctes. Nous n'avons pas autant de chance quand nous compter les façons de répartir les objets, distinguables ou impossibles à distinguer, en des boites; il n'y a pas de formules fermées à utiliser dans ces cas.

OBJETS DISTINCTIFS ET BOÎTES DISTINCTIVES Nous considérons d'abord
cas où des objets reconnaissables sont placés dans des boîtes reconnaissables. Prenons l'exemple 8
dans lequel les objets sont des cartes et les boîtes sont des mains de joueurs.

EXEMPLE 8 Combien y a-t-il de façons de distribuer des mains de 5 cartes à chacun des quatre joueurs de la norme
jeu de 52 cartes?

Solution: nous utiliserons la règle du produit pour résoudre ce problème. Pour commencer, notez que le premier joueur
peut recevoir 5 cartes de la manière $C(52, 5)$. Le deuxième joueur peut recevoir 5 cartes de façon $C(47, 5)$,
car il ne reste que 47 cartes. Le troisième joueur peut recevoir 5 cartes de façon $C(42, 5)$. Finalement,
le quatrième joueur peut recevoir 5 cartes de façon $C(37, 5)$. Par conséquent, le nombre total de façons de traiter
quatre joueurs 5 cartes chacun est

$$C(52, 5)\, C(47, 5)\, C(42, 5)\, C(37, 5) = \frac{52!}{47!\,5!} \cdot \frac{47!}{42!\,5!} \cdot \frac{42!}{37!\,5!} \cdot \frac{37!}{32!\,5!}$$

$$= \frac{52!}{5!\,5!\,5!\,5!\,32!}.$$

▲

Remarque: La solution de l'exemple 8 est égale au nombre de permutations de 52 objets, avec 5
des objets distinctifs de chacun des quatre types différents et 32 objets d'un cinquième type. Cette égalité
peut être vu en définissant une correspondance biunivoque entre les permutations de ce type et la dis-
tributions de cartes aux joueurs. Pour définir cette correspondance, commandez d'abord les fiches de 1 à 52.
Ensuite, les cartes distribuées au premier joueur correspondent aux cartes dans les positions attribuées aux objets de
le premier type de la permutation. De même, les cartes distribuées aux deuxième, troisième et quatrième joueurs,
respectivement, correspondent à des cartes dans les positions attribuées aux objets des deuxième, troisième et quatrième
type, respectivement. Les cartes qui ne sont distribuées à aucun joueur correspondent à des cartes dans les positions attribuées
aux objets du cinquième type. Le lecteur doit vérifier qu'il s'agit d'une correspondance biunivoque.

L'exemple 8 est un problème typique qui implique la distribution d'objets reconnaissables
boîtes à colorier. Les objets distinguables sont les 52 cartes, et les cinq identifiables
les boîtes sont les mains des quatre joueurs et du reste du jeu. Compter les problèmes qui impliquent
la distribution d'objets reconnaissables dans des boîtes peut être résolue en utilisant le théorème 4.

THÉORÈME 4 Le nombre de façons de distribuer n objets distinguables dans k cases distinctes afin
que n_i objets sont placés dans la case i, $i = 1, 2, ..., k$, est égal à

$$\frac{n!}{n_1!\, n_2! \cdots n_k!}.$$

Le théorème 4 peut être prouvé en utilisant la règle du produit. Nous laissons les détails à l'exercice 47. Il peut également
être prouvée (voir exercice 48) en établissant une correspondance biunivoque entre les permutations
compté par le théorème 3 et les façons de distribuer les objets comptés par le théorème 4.

OBJETS ET BOÎTES indiscernables distinguables compter les
nombre de façons de placer n objets indiscernables dans k boîtes distinctes se révèle
revient à compter le nombre de n -combinaisons pour un ensemble avec k éléments lors de la répétition
sont autorisées. La raison derrière cela est qu'il existe une correspondance biunivoque entre

n -combinaisons d'un ensemble avec k éléments lorsque la répétition est autorisée et les façons de placer
n boules indiscernables dans k boîtes distinctes. Pour mettre en place cette correspondance, nous avons mis un
balle dans le i ème bac chaque fois que le i ème élément de l'ensemble est inclus dans la n- combinaison.

EXEMPLE 9 Combien de façons y a-t-il de placer 10 balles indiscernables dans huit cases distinctes?

Solution: Le nombre de façons de placer 10 boules indiscernables dans huit bacs est égal au nombre
ber de 10 combinaisons d'un ensemble de huit éléments lorsque la répétition est autorisée. Par conséquent,
il y a

$$C(8 + 10 - 1, 10) = C(17, 10) = \frac{17!}{10!\,7!} = 19, 448.$$

▲

Cela signifie qu'il existe $C(n + r - 1, n - 1)$ façons de placer r objets indiscernables
dans n boîtes distinctes.

OBJETS DISTINCTIFS ET BOÎTES INDISTINGUABLES Compter les voies
placer n objets *reconnaissables* dans k boîtes indiscernables est plus difficile que de compter
les façons de placer des objets, des objets distincts ou indiscernables, dans des objets

des boites. Nous illustrons cela avec un exemple.

EXEMPLE 10 De combien de façons existe-t-il de placer quatre employés différents dans trois bureaux indiscernables, quand chaque bureau peut contenir un nombre illimité d'employés?

Solution: Nous allons résoudre ce problème en énumérant toutes les façons dont ces employés peuvent être placés dans les bureaux. Nous représentons les quatre employés par A, B, C et D. Tout d'abord, nous notons que nous pouvons répartir les employés de sorte que tous les quatre soient regroupés dans un seul bureau, trois dans un même bureau et un quatrième est placé dans un deuxième bureau, deux employés sont placés dans un bureau et deux dans un deuxième bureau, et enfin, deux sont placés dans un bureau, et un chacun dans les deux autres bureaux. Chaque façon de répartir ces employés dans ces bureaux peut être représentée par un moyen de partitionner les éléments A, B, C et D en sous-ensembles disjoints.

Nous pouvons regrouper les quatre employés dans un même bureau de la même manière, représentés par $\{\{A, B, C, D\}\}$. Nous pouvons mettre trois employés dans un bureau et le quatrième employé dans un bureau différent de quatre façons exactement, représenté par $\{\{A, B, C\}, \{D\}\}$, $\{\{A, B, D\}, \{C\}\}$, $\{\{A, C, D\}, \{B\}\}$ et $\{\{B, C, D\}, \{A\}\}$. Nous pouvons mettre deux employés dans un bureau et deux dans un deuxième bureau de trois façons exactement, représenté par $\{\{A, B\}, \{C, D\}\}$, $\{\{A, C\}, \{B, D\}\}$, et $\{\{A, D\}, \{B, C\}\}$. Enfin, nous pouvons mettre deux employés dans un bureau, et un chacun dans chaque des deux bureaux restants de six façons, représentés par $\{\{A, B\}, \{C\}, \{D\}\}$, $\{\{A, C\}, \{B\}, \{D\}\}$, $\{\{A, D\}, \{B\}, \{C\}\}$, $\{\{B, C\}, \{A\}, \{D\}\}$, $\{\{B, D\}, \{A\}, \{C\}\}$ et $\{\{C, D\}, \{A\}, \{B\}\}$.

En comptant toutes les possibilités, nous constatons qu'il y a 14 façons de mettre quatre employés différents en trois bureaux indiscernables. Une autre façon de voir ce problème est de regarder le nombre des bureaux dans lesquels nous mettons des employés. Notez qu'il existe six façons de mettre quatre différents les employés dans trois bureaux indiscernables afin qu'aucun bureau ne soit vide, sept façons de mettre quatre différents employés dans deux bureaux indiscernables afin qu'aucun bureau ne soit vide, et à sens unique mettre quatre employés dans un bureau pour qu'il ne soit pas vide. ▲

Il n'y a pas de formule fermée simple pour le nombre de façons de distribuer n distinguable objets dans j boîtes indiscernables. Cependant, il existe une formule impliquant une sommation, que nous allons maintenant décrire. Soit $S(n, j)$ le nombre de façons de distribuer n distin- les objets pouvant en j boîtes indiscernable de sorte qu'aucune boîte est vide. Les nombres $S(n, j)$ sont appelé **nombres de Stirling du deuxième type**. Par exemple, l'exemple 10 montre que $S(4, 3) = 6$, $S(4, 2) = 7$, et $S(4, 1) = 1$. Nous voyons que le nombre de façons de distribuer n *se* distingue objets dans k cases indiscernables (où le nombre de cases non vides est égal à k, $k - 1, \ldots, 2$ ou 1) est égal à $\sum_{j=1}^{k} S(n, j)$. Par exemple, en suivant le raisonnement de l'exemple 10, le nombre de façons de répartir quatre objets reconnaissables dans trois boîtes indiscernables

est égal à $S(4, 1) + S(4, 2) + S(4, 3) = 1 + 7 + 6 = 14$. Utilisation du principe d'inclusion-exclusion (voir section 8.6), il peut être démontré que

$$S(n, j) = \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^i \binom{j}{i} (j - i)^n .$$

Par conséquent, le nombre de façons de répartir n objets distinguables en k indiscernables boîtes égale

$$\sum_{j=1}^{k} S(n, j) = \sum_{j=1}^{k} \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^i \binom{j}{i} (j - i)^n .$$

Remarque: Le lecteur peut être curieux au sujet des nombres de Stirling du premier type. Une combinatoire définition des **nombres de Stirling sans signe du premier type**, les valeurs absolues de Stirling numéros du premier type, se trouvent dans le préambule de l'exercice 47 du Supplément Des exercices. Pour la définition des nombres de Stirling du premier type, pour plus d'informations sur Numéros de Stirling du deuxième type, et pour en savoir plus sur les nombres de Stirling du premier type et la relation entre les nombres de Stirling du premier et du deuxième type, voir combinatoire des manuels tels que [Bó07], [Br99] et [RoTe05], et le chapitre 6 dans [MiRo91].

OBJETS INDISTINGUABLES ET BOÎTES INDISTINGUABLES Quelques comptages les problèmes peuvent être résolus en déterminant le nombre de façons de distribuer les objets indiscernables dans des boîtes indiscernables. Nous illustrons ce principe avec un exemple.

EXEMPLE 11 Combien y a-t-il de façons d'emballer six exemplaires du même livre dans quatre boîtes identiques, où une boîte peut contenir jusqu'à six livres?

Solution: Nous énumérerons toutes les façons d'emballer les livres. Pour chaque façon d'emballer les livres, nous lister le nombre de livres dans la case avec le plus grand nombre de livres, suivi des nombres de livres dans chaque boîte contenant au moins un livre, par ordre décroissant de livres dans un boîte. Les façons dont nous pouvons emballer les livres sont

6
5 , 1
4 , 2
4 , 1 , 1
3 , 3
3 , 2 , 1
3 , 1 , 1 , 1
2 , 2 , 2
2 , 2 , 1 , 1.

Par exemple, 4 , 1 , 1 indique qu'une boîte contient quatre livres, une deuxième boîte contient un seul livre, et une troisième boîte contient un seul livre (et la quatrième boîte est vide).Nous concluons que il y a neuf façons autorisées d'emballer les livres, car nous les avons toutes répertoriées. ▲

Observez que la distribution de n objets indiscernables dans k boîtes indiscernables est la comme écrire n comme la somme d'au plus k entiers positifs dans un ordre non croissant. Si $un_1 + un_2 + \cdots + a_j = n$, où a_1 , a_2 , ..., a_j sont des entiers positifs avec $a_1 \geq a_2 \geq \cdots \geq a_j$, on dit que a_1 , a_2 , ..., a_j est une **partition** de l'entier positif n en j entiers positifs. On voit que si $p_k(n)$ est le nombre de partitions de n en au plus k entiers positifs, alors il y a $p_k(n)$ façons de répartissez n objets indiscernables dans k boîtes indiscernables. Pas de formule fermée simple existe pour ce numéro. Pour plus d'informations sur les partitions d'entiers positifs, voir [Ro11].

Des exercices

1. De combien de manières différentes peut-on sélectionner cinq éléments dans l'ordre à partir d'un ensemble de trois éléments lorsque la répétition est permis?

2. De combien de manières différentes peut-on sélectionner cinq éléments dans l'ordre à partir d'un ensemble de cinq éléments lorsque la répétition est permis?

3. Combien y a-t-il de chaînes de six lettres?

4. Chaque jour, un étudiant choisit au hasard un sandwich pour déjeuner à partir d'un tas de sandwichs enveloppés. S'il y en a six sortes de sandwichs, combien de façons différentes existe-t-il pour que l'étudiant choisisse des sandwichs pour les sept jours d'une semaine si l'ordre dans lequel les sandwichs sont choisis importe?

5. De combien de façons existe-t-il pour attribuer trois emplois à cinq employés si chaque employé peut recevoir plus d'un emploi?

6. Combien de façons existe-t-il de sélectionner cinq éléments à partir d'un ensemble à trois éléments lorsque la répétition est permis?

7. Combien de façons existe-t-il de sélectionner trois éléments éléments d'un ensemble à cinq éléments lorsque la répétition est permis?

8. Combien de façons différentes de choisir une douzaine beignets des 21 variétés dans un magasin de beignets?

9. Une boutique de bagels propose des bagels à l'oignon, des bagels aux graines de pavot, des œufs bagels, bagels salés, bagels pumpernickel, graines de sésame bagels, bagels aux raisins et bagels nature. Combien de façons sont là pour choisir

a) six bagels?
b) une douzaine de bagels?
c) deux douzaines de bagels?
d) une douzaine de bagels avec au moins un de chaque type?
e) une douzaine de bagels avec au moins trois bagels aux œufs et aucun plus de deux bagels salés?

10. Un magasin de croissants a des croissants nature, des croissants cerises, croissants au chocolat, croissants aux amandes, croissants aux pommes, et croissants au brocoli. De combien de façons existe-t-il choisir

a) une douzaine de croissants?
b) trois douzaines de croissants?
c) deux douzaines de croissants avec au moins deux de chaque type?
d) deux douzaines de croissants avec pas plus de deux brocolis des croissants?
e) deux douzaines de croissants avec au moins cinq croissants au chocolat sants et au moins trois croissants aux amandes?
f) deux douzaines de croissants avec au moins un croissant nature,

12. Combien de combinaisons différentes de pièces de un cent, nickels, dimes, quarts et demi dollars peut une tirelire con- savoir si elle contient 20 pièces?

13. Un éditeur de livres possède 3 000 exemplaires d'un livre ics. Combien de façons existe-t-il de stocker ces livres dans leurs trois entrepôts si les exemplaires du livre sont indiscernable?

14. Combien de solutions y a-t-il à l'équation

$$x_1 + x_2 + x_3 + x_4 = 17 ,$$

où x_1 , x_2 , x_3 et x_4 sont des entiers non négatifs?

15. Combien de solutions y a-t-il à l'équation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 21 ,$$

où x_i , $i = 1 , 2 , 3 , 4 , 5$, est un entier non négatif tel cette

a) $x_1 \geq 1$?
b) $x_i \geq 2$ pour $i = 1 , 2 , 3 , 4 , 5$?
c) $0 \leq x_1 \leq 10$?
d) $0 \leq x_1 \leq 3$, $1 \leq x_2 < 4$ et $x_3 \geq 15$?

16. Combien de solutions y a-t-il à l'équation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 29 ,$$

où x_i , $i = 1 , 2 , 3 , 4 , 5 , 6$, est un entier non négatif tel cette

a) $x_i > 1$ pour $i = 1 , 2 , 3 , 4 , 5 , 6$?
b) $x_1 \geq 1$, $x_2 \geq 2$, $x_3 \geq 3$, $x_4 \geq 4$, $x_5 > 5$ et $x_6 \geq 6$?
c) $x_1 \leq 5$?
d) $x_1 < 8$ et $x_2 > 8$?

17. Combien de chaînes de 10 chiffres ternaires (0, 1 ou 2) y a-t-il qui contiennent exactement deux 0, trois 1 et cinq 2?

18. Combien de chaînes de 20 décimales existe-t-il qui tain deux 0s, quatre 1s, trois 2s, un 3, deux 4s, trois 5s, deux 7 et trois 9?

19. Supposons qu'une famille nombreuse ait 14 enfants, dont deux des ensembles de triplets identiques, trois ensembles de jumeaux identiques et deux enfants individuels. Combien de façons de s'asseoir ces enfants dans une rangée de chaises si les triplets identiques ou les jumeaux ne peuvent pas être distingués les uns des autres?

20. Combien de solutions existe-t-il à l'inégalité

$$x_1 + x_2 + x_3 \leq 11 ,$$

où x_1 , x_2 et x_3 sont des entiers non négatifs? [*Indice:* en- troduire une variable auxiliaire x_4 telle que $x_1 + x_2 + x_3 + x_4 = 11$.]

21. De combien de façons existe-t-il de distribuer six balles capables dans neuf bacs reconnaissables?

22. De combien de façons existe-t-il de distribuer 12 des balles capables dans six bacs distincts?

au moins deux croissants aux cerises, au moins trois croissants tardifs, au moins un croissant aux amandes, au moins deux croissants aux pommes et pas plus de trois brocolis des croissants?

11. De combien de façons existe-t-il pour choisir huit pièces tirelire contenant 100 pièces identiques et 80 iden- nickels tical?

23. Combien de façons existe-t-il de distribuer 12 objets dans six boîtes distinctes de sorte que deux objets sont placés dans chaque boîte?

24. Combien de façons existe-t-il de distribuer 15 objets dans cinq boîtes distinctes de sorte que le les boîtes contiennent un, deux, trois, quatre et cinq objets, respectivement.

25. Combien d'entiers positifs inférieurs à 1 000 000 ont la somme de leurs chiffres égale à 19?

26. Combien d'entiers positifs inférieurs à 1 000 000 ont en fait un chiffre égal à 9 et avoir une somme de chiffres égale à 13?

27. Il y a 10 questions sur une finale mathématique discrète examen. Combien de façons existe-t-il d'attribuer des scores problèmes si la somme des scores est de 100 et chaque question vaut au moins 5 points?

28. Montrer qu'il y a $C(n + r - q_1 - q_2 - \cdots - q_r - 1, n - q_1 - q_2 - \cdots - q_r)$ sélection non ordonnée différente tions de n objets de r types différents qui incluent à moins q_1 objets de type un, q_2 objets de type deux , ..., et q_r objets de type r .

29. Combien de chaînes de bits différentes peuvent être transmises si la chaîne doit commencer par 1 bit, doit comprendre trois 1 bits supplémentaires (de sorte qu'un total de quatre 1 bits soit envoyé), doit comprendre un total de 12 0 bits et doit avoir au moins deux 0 bits suivant chaque 1 bit?

30. Combien de chaînes différentes peuvent être faites à partir des lettres à *MISSISSIPPI* , en utilisant toutes les lettres?

31. Combien de chaînes différentes peuvent être faites à partir des lettres en *ABRACADABRA* , en utilisant toutes les lettres?

32. Combien de chaînes différentes peuvent être faites à partir des lettres dans *AARDVARK* , en utilisant toutes les lettres, si les trois *A* doivent être consécutif?

33. Combien de chaînes différentes peuvent être faites à partir des lettres à *ORONO* , en utilisant tout ou partie des lettres?

34. Combien de chaînes de cinq caractères ou plus peuvent être formé à partir des lettres de *SEERESS* ?

35. Combien de chaînes de sept caractères ou plus peuvent être formé à partir des lettres *EVERGREEN* ?

36. Combien de chaînes de bits différentes peuvent être formées en utilisant six 1 et huit 0?

37. Un élève a trois mangues, deux papayes et deux kiwis des fruits. Si l'élève mange un fruit chaque jour, et seul le type de fruit compte, de combien de façons différentes ces fruits peuvent-ils être consommés?

38. Une professeure emballe sa collection de 40 numéros d'un journal des matiques en quatre boîtes avec 10 numéros par boîte. Comment de nombreuses façons peut-elle distribuer les journaux si

a) chaque case est numérotée de façon à ce qu'elles soient capable?

b) les cases sont identiques, de sorte qu'elles ne peuvent pas être guished?

39. Combien de façons de voyager dans l' espace *xyz à* partir du origine $(0, 0, 0)$ au point $(4, 3, 5)$ en effectuant les étapes un unité dans le sens x positif , une unité dans le y positif ou une unité dans la direction z positive ? (En mouvement dans le sens négatif x , y ou z est interdit, de sorte que aucun retour en arrière n'est autorisé.)

40. Combien y a-t-il de façons de voyager dans l' espace *xyzw* depuis l'origine $(0, 0, 0, 0)$ au point $(4, 3, 5, 4)$ en prenant étapes d'une unité dans le x positif, y positif, z positif ou direction w positive ?

41. Combien de façons existe-t-il de distribuer les mains de sept cartes chacun des cinq joueurs d'un jeu standard de 52 cartes?

42. En bridge, les 52 cartes d'un deck standard sont distribuées à quatre joueurs. Combien de façons différentes de gérer le pont mains à quatre joueurs?

43. Combien de façons existe-t-il de distribuer les mains de cinq cartes chacun des six joueurs d'un deck contenant 48 différents cartes?

44. De combien de façons une douzaine de livres peuvent-ils être placés sur quatre étagères distinctes

a) si les livres sont des copies identiques des mêmes Titre?

b) s'il n'y a pas deux livres identiques et les positions des des livres sur les étagères sont importants? [*Indice:* divisez cela en 12 tâches, en plaçant chaque livre séparément. Commencez avec le séquence 1, 2, 3, 4 pour représenter les étagères. Représenter envoyé les livres par b_i , $i = 1, 2, ..., 12$. Placez b_1 au à droite de l'un des termes 1, 2, 3, 4. Puis successivement placer b_2, b_3, ... et b_{12}.]

45. De combien de façons n livres placés sur k distin- étagères en mesure

a) si les livres sont des copies identiques des mêmes Titre?

b) s'il n'y a pas deux livres identiques et les positions des des livres sur les étagères sont importants?

46. Une étagère contient 12 livres d'affilée. Combien de façons là pour choisir cinq livres afin qu'il n'y ait pas deux livres adjacents sont choisis? [*Astuce:* Représentez les livres choisis par les bars et les livres non choisis par les stars. Comptez le nombre de séquences de cinq barres et sept étoiles de sorte que pas deux les barres sont adjacentes.]

∗ **47.** Utilisez la règle du produit pour prouver le théorème 4, en plaçant d'abord objets dans la première case, puis en plaçant des objets dans la seconde boîte, et ainsi de suite.

∗ **48.** Prouvez le théorème 4 en mettant d'abord en place un cor- réponse entre permutations de n objets avec n_i objets indiscernables de type i , $i = 1, 2, 3, ..., k$ et les distributions de n objets dans k cases telles que n_i ob- jets sont placés dans la case i , $i = 1, 2, 3, ..., k$ puis ap- appliquer le théorème 3.

∗ **49.** Dans cet exercice, nous allons prouver le théorème 2 en établir une correspondance biunivoque entre l'ensemble de combinaisons r avec répétition autorisée de $S = \{1, 2, 3, ..., n\}$ et l'ensemble des r -combinaisons de l'ensemble $T = \{1, 2, 3, ..., n + r - 1\}$.

a) Disposez les éléments en une combinaison r , avec etition permise, de S dans une séquence croissante $x_1 \leq x_2 \leq \cdots \leq x_r$. Montrer que la séquence s'est formée en ajoutant $k - 1$ au k ème terme est strictement croissant. Conclure que cette séquence est composée de r distincts des éléments de T .

b) Montrer que la procédure décrite en (a) définit une correspondance biunivoque entre l'ensemble des r -combinaisons, avec répétition autorisée, de S et la r -ensembles composés de T . [*Astuce:* Montrez la correspondance la spondence peut être inversée en associant au r - combinaison $\{x_1, x_2, ..., x_r\}$ de T , avec $1 \leq x_1 < x_2 < \cdots < x_r \leq n + r - 1$, la combinaison r avec répétition permise de S , formée en soustrayant k - 1 du k ème élément.]

c) Conclure qu'il y a $C(n + r - 1, r)$ r - combinaisons avec répétition autorisées à partir d'un ensemble avec n éléments.

50. De combien de façons existe-t-il de distribuer cinq objets capables dans trois boîtes indiscernables?

51. De combien de façons existe-t-il de distribuer six objets dans quatre boîtes indiscernables de sorte que chacun des les boîtes contiennent au moins un objet?

52. De combien de façons existe-t-il de mettre cinq ees dans quatre bureaux identiques?

53. De combien de façons y a-t-il six emplois temporaires dans quatre bureaux identiques afin qu'il y ait au moins un employé temporaire dans chacun de ces quatre bureaux?

54. De combien de façons existe-t-il de distribuer cinq objets capables dans trois boîtes indiscernables?

55. De combien de façons existe-t-il de distribuer six objets capables dans quatre boîtes indiscernables de sorte que chaque des boîtes contient au moins un objet?

56. Combien y a-t-il de façons d'emballer huit DVD identiques en cinq boîtes indiscernables afin que chaque boîte contienne au moins un DVD?

57. Combien y a-t-il de façons d'emballer neuf DVD identiques dans trois boîtes indiscernables afin que chaque boîte contienne contient au moins deux DVD?

58. Combien y a-t-il de façons de distribuer cinq balles sept cases si chaque case doit avoir au plus une balle en elle si

a) les balles et les boîtes sont étiquetées?

b) les boules sont étiquetées, mais les boîtes ne sont pas étiquetées?

c) les boules ne sont pas étiquetées, mais les boîtes sont étiquetées?

d) les balles et les boîtes sont sans étiquette?

59. Combien y a-t-il de façons de distribuer cinq balles en trois boîtes si chaque boîte doit contenir au moins une balle si

a) les balles et les boîtes sont étiquetées?

b) les boules sont étiquetées, mais les boîtes ne sont pas étiquetées?

c) les boules ne sont pas étiquetées, mais les boîtes sont étiquetées?

d) les balles et les boîtes sont sans étiquette?

60. Supposons qu'une ligue de basket-ball compte 32 équipes, réparties en deux conférences de 16 équipes chacune. Chaque conférence est divisé en trois divisions. Supposons que le centre nord La division compte cinq équipes. Chacune des équipes du Nord La division centrale joue quatre matchs contre chacun des d'autres équipes de cette division, trois matchs contre chacun des les 11 équipes restantes dans la conférence, et deux matchs contre chacune des 16 équipes de l'autre conférence. Dans combien d'ordres différents les jeux de l'un des les équipes de la division centrale du Nord soient-elles programmées?

∗ **61.** Supposons qu'un inspecteur d'armes doit inspecter chacun cinq sites différents deux fois, visitant un site par jour. le inspecteur est libre de sélectionner l'ordre dans lequel visiter ces mais ne peut pas visiter le site X, le site le plus suspect, sur deux jours consécutifs. Dans combien de commandes différentes peuvent l'inspecteur visite ces sites?

62. Combien de termes différents existe-t-il dans l'expansion de $(x_1 + x_2 + \cdots + x_m)^n$ après tout termes avec des ensembles identiques des exposants sont ajoutés?

∗ **63.** Démontrer le **théorème multinomial:** si n est un **entier** positif ger, alors

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{n_1 + n_2 + \cdots + n_m = n} C(n; n_1, n_2, \ldots, n_m)\, x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m},$$

où

$$C(n; n_1, n_2, \ldots, n_m) = \frac{n!}{n_1!\, n_2! \cdots n_m!}$$

est un **coefficient multinomial** .

64. Trouvez l'expansion de $(x + y + z)^4$.

65. Trouvez le coefficient de $x^3 y^2 z^5$ dans $(x + y + z)^{10}$.

66. Combien de termes y a-t-il dans l'expansion de $(x + y + z)^{100}$?

Génération de permutations et de combinaisons

introduction

Les méthodes de comptage de divers types de permutations et de combinaisons ont été décrites dans le sections précédentes de ce chapitre, mais parfois des permutations ou des combinaisons doivent être pas seulement compté. Considérez les trois problèmes suivants. Supposons d'abord qu'un vendeur doit visiter six villes différentes. Dans quel ordre ces villes doivent-elles être visitées pour minimiser le total temps de voyage? Une façon de déterminer le meilleur ordre est de déterminer le temps de trajet pour chacun des 6! = 720 ordres différents dans lesquels les villes peuvent être visitées et choisissez celle avec le plus petit temps de voyage. Deuxièmement, supposons que l'on nous donne un ensemble de six entiers positifs et souhaitons trouver un sous-ensemble d'entre eux qui a 100 comme somme, si un tel sous-ensemble existe. Une façon de trouver ces chiffres est de générer tous les $2^6 = 64$ sous-ensembles et vérifier la somme de leurs éléments. Troisièmement, supposons qu'un laboratoire compte 95 employés. Un groupe de 12 de ces employés avec un ensemble particulier de 25 compétences est nécessaire pour un projet. (Chaque employé peut avoir une ou plusieurs de ces compétences.) Une façon de trouver un tel ensemble d’employés consiste à générer tous les ensembles de 12 de ces employés et à vérifier s’ils les compétences souhaitées. Ces exemples montrent qu’il est souvent nécessaire de générer des permutations et combinaisons pour résoudre les problèmes.

Génération de permutations

Tout ensemble avec n éléments peut être placé en correspondance biunivoque avec l'ensemble $\{1, 2, 3, ..., n\}$. Nous pouvons lister les permutations de tout ensemble de n éléments en générant les permutations des n les plus petits entiers positifs, puis en remplaçant ces entiers par les éléments correspondants. De nombreux algorithmes différents ont été développés pour générer le $n!$ permutations de cet ensemble. nous décrira l'un d'entre eux qui est basé sur l'ordre **lexicographique** (ou **dictionnaire)** de l'ensemble des permutations de $\{1, 2, 3, ..., n\}$. Dans cet ordre, la permutation $a_1 a_2 \cdots a_n$ précède la permutation de $b_1 b_2 \cdots b_n$, si pour certains k, avec $1 \leq k \leq n$, $a_1 = b_1$, $a_2 = b_2$, ..., $a_{k-1} = b_{k-1}$, et $a_k < b_k$. En d'autres termes, une permutation de l'ensemble des n plus petits entiers positifs précède (dans l'ordre lexicographique) une deuxième permutation si le nombre dans cette permutation dans la première position où les deux permutations sont en désaccord est inférieure au nombre dans cette position dans le deuxième permutation.

EXEMPLE 1 La permutation 23415 de l'ensemble $\{1, 2, 3, 4, 5\}$ précède la permutation 23514, car ces permutations s'accordent dans les deux premières positions, mais le nombre dans la troisième position dans la première la permutation, 4, est inférieure au nombre en troisième position dans la deuxième permutation, 5. De même, la permutation 41532 précède 52143. ▲

Un algorithme pour générer les permutations de $\{1, 2, ..., n\}$ peut être basé sur une procédure procédure qui construit la permutation suivante dans l'ordre lexicographique suivant une permutation donnée $a_1 a_2 \cdots a_n$. Nous montrerons comment cela peut être fait. Supposons d'abord que $a_{n-1} < a_n$. Échangez un $_{n-1}$ et a_n pour obtenir une permutation plus grande. Aucune autre permutation n'est à la fois plus grande que la permutation et inférieure à la permutation obtenue en échangeant un $_{n-1}$ et un $_n$. Par exemple, la permutation suivante la plus grande après 234156 est 234165. Par contre, si $a_{n-1} > a_n$, alors a une permutation plus importante ne peut pas être obtenue en échangeant ces deux derniers termes dans la permutation. Regardez les trois derniers entiers de la permutation. Si $a_{n-2} < a_{n-1}$, alors les trois derniers entiers de la permutation peut être réorganisée pour obtenir la permutation suivante la plus grande. Mettez le plus petit des deux entiers a_{n-1} et un $_n$ qui est supérieure à une $_{n-2}$ en position $n - 2$. Ensuite, placer le restant entier et un $_{n-2}$ dans les deux dernières positions dans l'ordre croissant. Par exemple, le prochain plus grand la permutation après 234165 est 234516.

En revanche, si $a_{n-2} > a_{n-1}$ (et $a_{n-1} > a_n$), alors une permutation plus grande ne peut être obtenu en permutant les trois derniers termes de la permutation. Sur la base de ces observations, un une méthode générale peut être décrite pour produire la prochaine permutation plus grande dans l'ordre croissant suivant une permutation donnée $a_1 a_2 \cdots a_n$. Tout d'abord, trouvez les entiers a_j et a_{j+1} avec $a_j < a_{j+1}$ et

$$a_{j+1} > a_{j+2} > \cdots > a_n,$$

c'est-à-dire la dernière paire d'entiers adjacents dans la permutation où le premier entier de la paire est plus petit que le second. Ensuite, la permutation plus grande suivante dans l'ordre lexicographique est obtenue en mettant en j ème position le plus petit entier parmi a_{j+1}, a_{j+2}, ..., et a_n plus grand que a_j et listant dans l'ordre croissant le reste des entiers a_j, a_{j+1}, ..., a_n aux positions $j + 1$ à n. Il est facile de voir qu'il n'y a pas d'autre permutation plus grande que la permutation $a_1 a_2 \cdots a_n$ mais plus petit que la nouvelle permutation produite. (La vérification de ce fait est laissée comme un exercice pour le lecteur.)

EXEMPLE 2 Quelle est la prochaine permutation dans l'ordre lexicographique après 362541?

Solution: La dernière paire d'entiers a_j et a_{j+1} où $a_j < a_{j+1}$ est $un_3 = 2$ et $un_4 = 5$. Le le plus petit entier à droite de 2 supérieur à 2 dans la permutation est$un_5 = 4$. Par conséquent, 4 est placé en troisième position. Ensuite, les entiers 2, 5 et 1 sont placés dans l'ordre dans les trois derniers positions, donnant 125 comme les trois dernières positions de la permutation. Par conséquent, la prochaine permutation est 364125. ▲

Pour produire le n ! permutations des entiers 1 , 2 , 3 , ..., n , commencent par les plus petites permu- dans l'ordre lexicographique, à savoir 123 ⋯ n , et appliquer successivement la procédure décrite pour produire la prochaine permutation plus grande de$n$! - 1 fois. Cela donne toutes les permutations de les n plus petits entiers dans l'ordre lexicographique.

EXEMPLE 3 Générer les permutations des entiers 1, 2, 3 dans l'ordre lexicographique.

Solution: commencez par 123. La permutation suivante est obtenue en échangeant 3 et 2 pour obtenir 132. Ensuite, parce que 3 > 2 et 1 < 3, permutez les trois nombres entiers en 132. Mettez le plus petit de 3 et 2 dans la première position, puis mettez 1 et 3 dans l'ordre croissant dans les positions 2 et 3 pour obtenir 213. Il est suivi de 231, obtenu en échangeant 1 et 3, car 1< 3. La prochaine une permutation plus grande a 3 en première position, suivi de 1 et 2 dans l'ordre croissant, à savoir, 312. Enfin, échangez 1 et 2 pour obtenir la dernière permutation, 321. Nous avons généré le permutations de 1, 2, 3 dans l'ordre lexicographique. Ils sont 123, 132, 213, 231, 312 et 321. ▲

L'algorithme 1 affiche la procédure pour trouver la prochaine permutation dans l'ordre lexicographique après une permutation qui n'est pas nn - 1 n - 2 ... 2 1, qui est la plus grande permutation.

ALGORITHME 1 Génération de la permutation suivante dans l'ordre lexicographique.

procédure *permutation suivante* ($a_1 a_2 \ldots a_n$: permutation de
{1 , 2 , ..., n } différent de nn - 1 ... 2 1)
$j := n - 1$
tandis que $a_j > a_{j+1}$
  $j := j - 1$
{ j est le plus grand indice avec $un_j < a_{j+1}$ }
$k := n$
tandis que $a_j > a_k$
  $k := k - 1$
{ A_k est le plus petit nombre entier plus grand que d' un_j vers la droite de la_j }
échanger a_j et a_k
$r := n$
$s := j + 1$
tandis que $r > s$
  échanger un_r et un_s
  $r := r - 1$
  $s := s + 1$
{cela met la queue de la permutation après la j ème position dans l'ordre croissant}
{ $a_1 a_2 \ldots a_n$ est maintenant la prochaine permutation}

Génération de combinaisons

Comment générer toutes les combinaisons des éléments d'un ensemble fini?Parce qu'une combinaison n'est qu'un sous-ensemble, nous pouvons utiliser la correspondance entre des sous-ensembles de $\{a_1, a_2, ..., a_n\}$ et des chaînes de bits de longueur n.

Rappelons que la chaîne de bits correspondant à un sous-ensemble a un 1 en position k si a_k est dans le sous-ensemble, et a un 0 dans cette position si a_k n'est pas dans le sous-ensemble. Si toutes les chaînes de bits de longueur n peuvent être répertoriées, puis par la correspondance entre sous-ensembles et chaînes de bits, une liste de tous les sous-ensembles est obtenue.

Rappelons qu'une chaîne de bits de longueur n est également l'expansion binaire d'un entier compris entre 0 et $2^n - 1$. Les 2^n les chaînes de bits peuvent être répertoriées dans l'ordre de leur taille croissante sous forme d'entiers dans leur binaire extensions. Pour produire toutes les extensions binaires de longueur n, commencez par la chaîne de bits 000... 00, avec n zéros. Ensuite, trouvez successivement l'extension suivante jusqu'à ce que la chaîne de bits 111... 11 soit obtenue. À chaque étape, la prochaine expansion binaire est trouvée en localisant la première position de la droite qui est pas un 1, puis en changeant tous les 1 à droite de cette position en 0 et en faisant ce premier 0 (de à droite) a 1.

EXEMPLE 4 Recherchez la chaîne de bits suivante après 10 0010 0111.

Solution: le premier bit de droite qui n'est pas un 1 est le quatrième bit de droite. Changement ce bit à 1 et changez tous les bits suivants à 0s. Cela produit la prochaine chaîne de bits plus grande, 10 0010 1000. ▲

Procédure de production de la chaîne de bits suivante la plus grande après $b_{n-1} b_{n-2} \dots b_1 b_0$ est donné comme Algorithme 2.

ALGORITHME 2 Génération de la prochaine chaîne de bits plus grande.

procédure *chaîne de bits suivante* ($b_{n-1} b_{n-2} \dots b_1 b_0$: chaîne de bits non égale à 11... 11)
$i := 0$
tandis que $b_i = 1$
  $b_i := 0$
  $i := i + 1$
$b_i := 1$
{$b_{n-1} b_{n-2} \dots b_1 b_0$ est maintenant la chaîne de bits suivante}

Ensuite, un algorithme pour générer les r-combinaisons de l'ensemble $\{1, 2, 3, ..., n\}$ sera donné. Une combinaison r peut être représentée par une séquence contenant les éléments du sous-ensemble dans l'ordre croissant. Les combinaisons r peuvent être répertoriées en utilisant un ordre lexicographique sur ces séquences. Dans cet ordre lexicographique, la première combinaison r est $\{1, 2, ..., r - 1, r\}$ et la dernière combinaison r est $\{n - r + 1, n - r + 2, ..., n - 1, n\}$. La prochaine combinaison r après $a_1 a_2 \cdots a_r$ peut être obtenu de la manière suivante: Premièrement, localisez le dernier élément a_i dans le séquence telle que $a_i = n - r + i$. Ensuite, remplacez a_i par $a_i + 1$ et a_j par $a_i + j - i + 1$, pour $j = i + 1, i + 2, ..., r$. Il appartient au lecteur de montrer que cela produit le prochain plus grand r-combinaison dans l'ordre lexicographique. Cette procédure est illustrée par l'exemple 5.

EXEMPLE 5 Trouvez la prochaine combinaison plus grande de l'ensemble {1, 2, 3, 4, 5, 6} après {1, 2, 5, 6}.

Solution: Le dernier terme entre les termes d' a_i avec $a_1 = 1$, $a_2 = 2$, $a_3 = 5$, et $a_4 = 6$ de telle sorte que $a_i = 6 - 4 + i$ est $a_2 = 2$. Pour obtenir la combinaison 4 plus grande suivante, incrémentez a_2 par 1 pour obtenir $a_2 = 3$. Ensuite, définissez $a_3 = 3 + 1 = 4$ et $a_4 = 3 + 2 = 5$. Par conséquent, la combinaison 4 plus grande suivante est {1, 3, 4, 5}. ▲

L'algorithme 3 affiche le pseudocode pour cette procédure.

ALGORITHME 3 Génération de la prochaine combinaison *r* dans l'ordre lexicographique.

procédure *suivante combinaison r* ($\{a_1, a_2, ..., a_r\}$: sous-ensemble correct de $\{1, 2, ..., n\}$ différent de $\{n - r + 1, ..., n\}$ avec $a_1 < a_2 < \cdots < a_r$)
$i := r$
tandis que $a_i = n - r + i$
  $i := i - 1$
$a_i := a_i + 1$
pour $j := i + 1$ **à** r
  $a_j := a_i + j - i$
{$\{a_1, a_2, ..., a_r\}$ est maintenant la combinaison suivante}

Des exercices

1. Placez ces permutations de {1 , 2 , 3 , 4 , 5} en lexico-commande graphique: 43521, 15432, 45321, 23451, 23514, 14532, 21345, 45213, 31452, 31542.

2. Placez ces permutations de {1 , 2 , 3 , 4 , 5 , 6} en lexico-commande graphique: 234561, 231456, 165432, 156423, 543216, 541236, 231465, 314562, 432561, 654321, 654312, 435612.

3. Le nom d'un fichier dans un répertoire informatique se compose de trois lettres majuscules suivies d'un chiffre, où chaque la lettre est soit A, B ou C, et chaque chiffre est 1 ou 2. Répertoriez le nom de ces fichiers par ordre lexicographique, où nous classons les lettres en utilisant l'ordre alphabétique habituel des lettres.

4. Supposons que le nom d'un fichier dans un répertoire d'ordinateur se compose de trois chiffres suivis de deux lettres minuscules et chaque chiffre est 0, 1 ou 2, et chaque lettre est soit a soit b. Répertoriez le nom de ces fichiers par ordre lexicographique, où nous classons les lettres en utilisant l'ordre alphabétique habituel des lettres.

5. Trouvez la prochaine permutation plus grande dans l'ordre lexicographique après chacune de ces permutations.

a) 1432 **b)** 54123 **c)** 12453
d) 45231 **e)** 6714235 **f)** 31528764

6. Trouvez la prochaine permutation plus grande dans l'ordre lexicographique après chacune de ces permutations.

a) 1342 **b)** 45321 **c)** 13245
d) 612345 **e)** 1623547 **f)** 23587416

7. Utilisez l'algorithme 1 pour générer les 24 permutations du quatre premiers entiers positifs dans l'ordre lexicographique.

8. Utilisez l'algorithme 2 pour répertorier tous les sous-ensembles de l'ensemble {1 , 2 , 3 , 4}.

9. Utilisez l'algorithme 3 pour répertorier toutes les 3 combinaisons de {1 , 2 , 3 , 4 , 5}.

10. Montrer que l'algorithme 1 produit le permu- dans l'ordre lexicographique.

11. Montrez que l'algorithme 3 produit le prochain plus grand r -combinaison dans l'ordre lexicographique après une donnée r -combinaison.

12. Développer un algorithme pour générer les r- permutations d'un ensemble de n éléments.

13. Énumérez toutes les 3 permutations de {1 , 2 , 3 , 4 , 5}.

Les exercices restants de cette section développent une autre rithme de génération des permutations de $\{1, 2, 3, ..., n\}$. Cette L'algorithme est basé sur des extensions Cantor d'entiers. Chaque entier non négatif inférieur à n ! possède une extension Cantor unique sion

$$un_1 1! + a_2 2! + \cdots + a_{n-1} (n - 1) !$$

où a_i est un entier non négatif ne dépassant pas i , pour $i = 1, 2, ..., n - 1$. Les entiers $a_1, a_2, ..., a_{n-1}$ sont appelés **Chiffres de cantor** de cet entier.

Étant donné une permutation de $\{1, 2, ..., n\}$, soit a_{k-1}, $k = 2, 3, ..., n$, soit le nombre d'entiers inférieur à k qui suit k faible dans la permutation. Par exemple, dans la permutation 43215, a_1 est le nombre d'entiers inférieurs à 2 qui suivent faible 2, donc $a_1 = 1$. De même, pour cet exemple $a_2 = 2$, $a_3 = 3$, et $a_4 = 0$. Considérez la fonction de l'ensemble de permu- de $\{1, 2, 3, ..., n\}$ à l'ensemble des entiers non négatifs moins de n ! qui envoie une permutation à l'entier qui a $a_1, a_2, ..., a_{n-1}$, ainsi défini, comme ses chiffres de Cantor.

14. Trouvez les chiffres de Cantor $a_1, a_2, ..., a_{n-1}$ qui correspondent à ces permutations.

a) 246531 **b)** 12345 **c)** 654321

15. Montrer que la correspondance décrite dans le préambule est une bijection entre l'ensemble des permutations de $\{1, 2, 3, ..., n\}$ et les entiers non négatifs inférieurs à n !.

16. Trouvez les permutations de {1 , 2 , 3 , 4 , 5} qui correspondent à ces nombres entiers par rapport à la correspondance entre expansions et permutations Cantor comme décrit dans le préambule de l'exercice 14.

a) 3 **b)** 89 **c)** 111

17. Développer un algorithme pour produire toutes les permutations d'un ensemble de n éléments basés sur la correspondance décrite dans le préambule de l'exercice 14.

Termes et résultats clés

TERMES

combinatoire: l'étude des arrangements d'objets
énumération: le comptage des arrangements d'objets
diagramme d'arbre: un diagramme composé d'une racine, laissant des branches la racine et d'autres branches laissant certains des points de terminaison des succursales
permutation: une disposition ordonnée des éléments d'un ensemble
***r*- permutation:** un agencement ordonné de r éléments d'un ensemble
***P* (*n, r*):** le nombre de r- permutations d'un ensemble à n éléments
***r* -combination:** une sélection non ordonnée d'éléments r d'un ensemble
***C* (*n, r*):** le nombre de r -combinaisons d'un ensemble avec n éléments
coefficient binomial $\binom{n}{r}$ **:** aussi le nombre de r -combinaisons d'un ensemble avec n éléments
preuve combinatoire: une preuve qui utilise des arguments de comptage plutôt que la manipulation algébrique pour prouver un résultat
Le triangle de Pascal: une représentation des coefficients binomiaux cients où la i ème rangée du triangle contient $\binom{i}{j}$ pour $j = 0, 1, 2, ..., i$
***S* (*n, j*):** le nombre de Stirling du second type dénotant le nombre de façons de distribuer n objets distinctifs dans j boîtes indiscernables pour qu'aucune boîte ne soit vide
règle de soustraction pour le comptage ou **inclusion-exclusion pour ensembles:** si une tâche peut être effectuée de n_1 façons ou n_2 façons, alors le nombre de façons de faire la tâche est $n_1 + n_2$ moins le nombre de façons de faire la tâche qui sont communes à la deux manières différentes.
règle de soustraction ou **inclusion-exclusion pour les ensembles:** le nombre des éléments dans l'union de deux ensembles est la somme du nombre d'éléments dans ces ensembles moins le nombre d'éléments dans leur intersection.
règle de division pour le comptage: il existe n / d façons d'effectuer une tâche si cela peut être fait en utilisant une procédure qui peut être effectuée de n façons, et pour chaque façon w , exactement d des n voies correspondent à la voie w .
règle de division pour les ensembles: supposons qu'un ensemble fini A soit l'union de n sous-ensembles disjoints contenant chacun d éléments. Alors $n = | A | / d$.
le principe du pigeonhole: lorsque plus de k objets sont placé dans k boîtes, il doit y avoir une boîte contenant plus d'un objet.
le principe du pigeonnier généralisé: lorsque N objets sont placé dans k cases, il doit y avoir une case contenant au moins $\lceil N / k \rceil$ objets.

$$P(n, r) = \frac{n\,!}{(n - r)\,!}$$

RÉSULTATS

$$\binom{n}{\ } \qquad n\,!$$

règle de produit pour le comptage: le nombre de façons de procédure qui consiste en deux tâches est le produit du nombre des façons de faire la première tâche et le nombre de façons de faire la deuxième tâche après la première tâche.

règle de produit pour les ensembles: le nombre d'éléments dans la Le produit sien des ensembles finis est le produit du nombre de éléments dans chaque ensemble.

règle de somme pour le comptage: nombre de façons d'effectuer une tâche dans l'une des deux façons est la somme du nombre de façons de faire ces tâches si elles ne peuvent pas être effectuées simultanément.

règle de somme pour les ensembles: le nombre d'éléments dans l'union de ensembles finis disjoints par paire est la somme des nombres de éléments de ces ensembles.

$C(n, r) = r = r!\,(n-r)!$

L'identité de Pascal: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

le théorème binomial: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

Il y a n^r r- permutations d'un ensemble avec n éléments lorsque la répétition est autorisée.

Il existe des combinaisons $C(n+r-1, r)$ r d'un ensemble avec n éléments lorsque la répétition est autorisée.

Il y en a $n!/(n_1!\,n_2!\cdots n_k!)$ permutations de n objets de k types où il y a n_i objets indiscernables de type i pour $i = 1, 2, 3, \ldots, k$.

l'algorithme de génération des permutations de l'ensemble $\{1, 2, \ldots, n\}$

Questions de révision

1. Expliquez comment les règles de somme et de produit peuvent être utilisées pour trouver le nombre de chaînes de bits dont la longueur ne dépasse pas dix.

2. Expliquez comment trouver le nombre de chaînes de bits de longueur n'excédant pas 10 qui ont au moins un bit 0.

3. a) Comment la règle du produit peut-elle être utilisée pour trouver le numéro des fonctions d'un ensemble avec m éléments à un ensemble avec n éléments?

b) Combien de fonctions y a-t-il dans un ensemble de cinq éléments à un ensemble de 10 éléments?

Épisode 461

c) Comment la règle du produit peut-elle être utilisée pour trouver le numéro des fonctions biunivoque d'un ensemble de m éléments à un ensemble avec n éléments?

d) Combien de fonctions un à un y a-t-il dans un ensemble avec cinq éléments à un ensemble de 10 éléments?

e) Combien y a-t-il de fonctions sur un ensemble avec cinq éléments à un ensemble de 10 éléments?

4. Comment pouvez-vous trouver le nombre de résultats possibles éliminatoires entre deux équipes où la première équipe qui gagne quatre matchs remportent les séries éliminatoires?

5. Comment pouvez-vous trouver le nombre de chaînes de bits de longueur dix qui commencent par 101 ou se terminent par 010?

6. a) Énoncez le principe du pigeonnier.

b) Expliquez comment le principe du pigeonnier peut être utilisé pour montrer que parmi 11 nombres entiers, au moins deux doivent avoir le même dernier chiffre.

7. a) Énoncer le principe généralisé des trous de pigeonnier.

b) Expliquez comment le principe généralisé des trous être utilisé pour montrer que parmi 91 entiers, il existe au moins dix qui se terminent par le même chiffre.

8. a) Quelle est la différence entre une combinaison r et une r- permutation d'un ensemble à n éléments?

b) Dériver une équation qui relie le nombre de r -com- combinaisons et le nombre de r- permutations d'un ensemble avec n éléments.

c) De combien de façons existe-t-il pour sélectionner six élèves une classe de 25 pour faire partie d'un comité?

d) De combien de façons existe-t-il pour sélectionner six élèves une classe de 25 pour occuper six postes de direction différents sur un comité?

9. a) Qu'est-ce que le triangle de Pascal?

b) Comment peut-on produire une rangée du triangle de Pascal celui au dessus?

10. Qu'entend-on par preuve combinatoire d'une identité? En quoi une telle preuve est-elle différente d'une preuve algébrique?

11. Expliquez comment prouver l'identité de Pascal à l'aide d'une argument moral.

12. a) Énonce le théorème binomial.

b) Expliquer comment prouver le théorème binomial en utilisant un argument combinatoire.

c) Trouver le coefficient de $x^{100} y^{101}$ dans l'expansion de $(2x + 5$ ans $)^{201}$.

13. a) Explique comment trouver une formule pour le nombre de façons pour sélectionner r objets parmi n objets lorsque la répétition est autorisé et l'ordre n'a pas d'importance.

b) De combien de façons existe-t-il pour sélectionner une douzaine d'objets parmi des objets de cinq types différents si des objets du même type sont-ils indiscernables?

c) De combien de façons existe-t-il pour sélectionner une douzaine d'objets de ces cinq types différents s'il doit y avoir au moins trois objets du premier type?

d) De combien de façons existe-t-il pour sélectionner une douzaine d'objets de ces cinq types différents s'il ne peut y avoir plus de quatre objets du premier type?

e) De combien de façons existe-t-il pour sélectionner une douzaine d'objets de ces cinq types différents s'il doit y avoir au moins deux objets du premier type, mais pas plus de trois objets du deuxième type?

14. a) Soit n et r des entiers positifs. Expliquez pourquoi nombre de solutions de l'équation $x_1 + x_2 + \cdots + x_n = r$, où x_i est un entier non négatif pour $i = 1, 2, 3, \ldots, n$, est égal au nombre de combinaisons r d'un ensemble avec n éléments.

b) Combien y a-t-il de solutions en nombres entiers non négatifs à l'équation $x_1 + x_2 + x_3 + x_4 = 17$?

c) Combien de solutions en nombres entiers positifs existe-t-il pour l'équation dans la partie (b)?

15. a) Dériver une formule pour le nombre de permutations de n objets de k types différents, où il y a n_1 indis- objets pouvant être différenciés de type un, n_2 indiscernables objets de type deux, ..., et n_k objets indiscernables projets de type k.

b) De combien de façons existe-t-il pour ordonner les lettres mot *INDISCREETNESS* ?

16. Décrire un algorithme pour générer toutes les permutations de l'ensemble des n plus petits entiers positifs.

17. a) Combien y a-t-il de façons de distribuer les mains de cinq cartes à six joueurs d'un jeu standard de 52 cartes?

b) De combien de façons sont là pour distribuer n distin- objets capables dans k boîtes distinctes de sorte que n_i les objets sont placés dans la case i ?

18. Décrire un algorithme pour générer toutes les combinaisons de l'ensemble des n plus petits entiers positifs.

Exercices supplémentaires

1. De combien de façons existe-t-il pour choisir 6 articles parmi 10 éléments teints lorsque

2. De combien de façons existe-t-il pour choisir 10 articles parmi 6 dis- éléments teints lorsque

a) les éléments des choix sont ordonnés et la répétition est interdit?

b) les éléments des choix sont ordonnés et la répétition est permis?

c) les éléments dans les choix ne sont pas ordonnés et se répètent n'est pas autorisé?

d) les éléments dans les choix ne sont pas ordonnés et se répètent est autorisée?

a) les éléments des choix sont ordonnés et la répétition est interdit?

b) les éléments des choix sont ordonnés et la répétition est permis?

c) les éléments dans les choix ne sont pas ordonnés et se répètent n'est pas autorisé?

d) les éléments dans les choix ne sont pas ordonnés et se répètent est autorisée?

3. Un test contient 100 vraies / fausses questions. Combien de de différentes manières un étudiant peut-il répondre aux questions du test, si les réponses peuvent être laissées en blanc?

4. Combien de chaînes de longueur 10 commencent par 000 ou se terminent par 1111?

5. Combien de chaînes de bits de longueur 10 sur l'alphabet $\{ a, b, c \}$ ont exactement trois a s ou exactement quatre b s?

6. Les numéros de téléphone internes du système téléphonique sur un campus se compose de cinq chiffres, le premier chiffre n'étant pas égal à zéro. Combien de numéros différents peuvent être attribués dans ce système?

7. Un glacier a 28 saveurs différentes, 8 différentes sortes de sauce et 12 garnitures.

a) De combien de manières différentes un plat de trois boules faire de la crème glacée où chaque saveur peut être utilisée plus d'une fois et l'ordre des cuillères ne correspond pas matière?

b) Combien de types différents de petits coupes glacées existe-t-il si un petit sundae contient une boule de crème glacée, un sauce, et une garniture?

c) Combien de types différents de grandes coupes glacées existe-t-il si un grand sundae contient trois boules de crème glacée, où chaque saveur peut être utilisée plus d'une fois et l'ordre des boules n'a pas d'importance; deux types de sauce, où chaque sauce ne peut être utilisée qu'une seule fois et l'ordre des sauces n'a pas d'importance; et trois top-pings, où chaque garniture ne peut être utilisée qu'une seule fois et l'ordre des garnitures n'a pas d'importance?

8. Combien d'entiers positifs moins de 1000

a) a exactement trois chiffres décimaux?

b) avoir un nombre impair de chiffres décimaux?

c) avoir au moins un chiffre décimal égal à 9?

d) n'ont pas de chiffres décimaux impairs?

e) avoir deux chiffres décimaux consécutifs égaux à 5?

f) sont des palindromes (c'est-à-dire, lisez le même avant et en arrière)?

9. Lorsque les nombres de 1 à 1000 sont écrits en déci-notation mal, combien de chacun de ces chiffres sont utilisés?

a) 0 **b)** 1 **c)** 2 **d)** 9

10. Il y a 12 signes du zodiaque. Combien de personnes nécessaire pour garantir qu'au moins six de ces personnes ont le même signe?

11. Une entreprise de biscuits de fortune fait 213 fortunes différentes. Un étudiant mange dans un restaurant qui utilise les fortunes de ce société et donne à chaque client un biscuit de fortune à la fin d'un repas. Quel est le plus grand nombre possible de fois que l'étudiant peut manger au restaurant sans obtenir la même fortune quatre fois?

12. Combien de personnes sont nécessaires pour garantir qu'au moins deux sont nés le même jour de la semaine et dans le même mois (peut-être dans des années différentes)?

13. Montrez que, étant donné tout ensemble de 10 entiers positifs non au-delà de 50, il existe au moins deux éléments à cinq éléments différents sous-ensembles de cet ensemble qui ont la même somme.

14. Un paquet de cartes de baseball contient 20 cartes. Combien des forfaits doivent être achetés pour garantir que deux cartes ces packages sont identiques s'il y en a 550 au total différentes cartes?

15. a) Combien de cartes doivent être choisies dans un jeu standard de 52 cartes pour garantir qu'au moins deux des quatre les as sont choisis?

b) Combien de cartes doivent être choisies dans un jeu standard de 52 cartes pour garantir qu'au moins deux des quatre as et au moins deux des 13 types sont choisis?

c) Combien de cartes doivent être choisies dans un jeu standard de 52 cartes pour garantir qu'il y a au moins deux cartes du même genre?

d) Combien de cartes doivent être choisies dans un jeu standard de 52 cartes pour garantir qu'il y a au moins deux cartes de chacun des deux types différents?

∗ **16.** Montrer que dans tout ensemble de $n + 1$ entiers positifs ne dépassent pas-ing $2n$ il doit y en avoir deux qui sont relativement premiers.

∗ **17.** Montrer que dans une séquence de m entiers, il existe un ou termes plus consécutifs avec une somme divisible par m .

18. Montrez que si cinq points sont ramassés à l'intérieur d'un carré avec une longueur de côté de 2, puis au moins deux de ces les points ne sont pas plus loin que $\sqrt{2}$ à part.

19. Montrer que l'expansion décimale d'un nombre rationnel doit se répéter à partir d'un certain point.

20. Une fois qu'un ver informatique infecte un ordinateur personnel via un infecté, il envoie une copie de lui-même à 100 e-mails les adresses électroniques qu'il trouve dans la boîte aux lettres électronique sur cet ordinateur personnel. Quel est le nombre maximum d'ordinateurs différents cet ordinateur peut infecter dans le temps nécessaire pour que le message infecté soit transféré cinq fois?

21. De combien de façons existe-t-il pour choisir une douzaine de beignets 20 variétés

a) s'il n'y a pas deux beignets de la même variété?

b) si tous les beignets sont de la même variété?

c) s'il n'y a pas de restrictions?

d) s'il existe au moins deux variétés parmi la douzaine beignets choisis?

e) s'il doit y avoir au moins six beignets fourrés aux bleuets?

f) s'il ne peut y en avoir plus de six remplis de bleuets des beignets?

22. Trouvez n si

a) $P(n, 2) = 110$. **b)** $P(n, n) = 5040$.

c) $P(n, 4) = 12\,P(n, 2)$.

23. Trouvez n si

a) $C(n, 2) = 45$. **b)** $C(n, 3) = P(n, 2)$.

c) $C(n, 5) = C(n, 2)$.

24. Montrer que si n et r sont des entiers non négatifs et $n \geq r$, ensuite

$$P(n+1, r) = P(n, r)(n+1)/(n+1-r).$$

* **25.** Supposons que S soit un ensemble avec n éléments. Combien commandé les paires (A, B) sont telles que A et B sont des sous-ensembles de S avec $A \subseteq B$? [*Astuce:* montrer que chaque élément de S appartient à A, $B - A$ ou $S - B$.]

26. Donner une preuve combinatoire du corollaire 2 de la section 6.4 en établissant une correspondance entre les sous-ensembles d'un défini avec un nombre pair d'éléments et les sous-ensembles de cet ensemble avec un nombre impair d'éléments. [*Indice:* prenez un ement *un* dans l'ensemble. Mettre en place la correspondance en mettant *un* dans le sous-ensemble s'il n'est pas déjà dedans et le retirer s'il est dans le sous-ensemble.]

27. Soit n et r *des* entiers avec $1 \leq r < n$. Montre CA

$$C(n, r-1) = C(n+2, r+1) - 2C(n+1, r+1) + C(n, r+1).$$

28. Prouver en utilisant l'induction mathématique que $\sum_{j=2}^{n} C(j, 2) = C(n+1, 3)$ chaque fois que n est un entier supérieur à 1.

29. Montrer que si n est un entier alors

$$\sum_{k=0}^{n} 3^k \binom{n}{k} = 4^n.$$

30. Montrez que $\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} 1 = \binom{n}{2}$ si n est un entier avec $n \geq 2$.

31. Montrez que $\sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} 1 = \binom{n}{3}$ si n est un teger avec $n \geq 3$.

32. Dans cet exercice, nous allons dériver une formule pour la somme de les carrés des n plus petits entiers positifs. Nous allons compter le nombre de triplets (i, j, k) où i, j et k sont entiers tels que $0 \leq i < k$, $0 \leq j < k$ et $1 \leq k \leq n$ de deux façons.

a) Montrer qu'il existe k^2 de ces triplets avec un k fixe . Déduce qu'il y a $\sum_{k=1}^{n} k^2$ de tels triplets.

b) Montrer que le nombre de ces triplets avec $0 \leq i < j < k$ et le nombre de ces triplets avec $0 \leq j < i < k$ égal à $C(n+1, 3)$.

c) Montrer que le nombre de ces triplets avec $0 \leq i = j < k$ est égal à $C(n+1, 2)$.

d) Combiner la partie (a) avec les parties (b) et (c), conclure cette

$$\sum_{k=1}^{n} k^2 = 2C(n+1, 3) + C(n+1, 2) = n(n+1)(2n+1)/6.$$

* **33.** Combien de chaînes de bits de longueur n, où $n \geq 4$, contiennent exactement deux occurrences de 01?

34. Soit S un ensemble. Nous disons qu'une collection de ensembles $A_1, A_2, \ldots, A_n$ contenant chacun d éléments, où $d \geq 2$, est *bicolore* s'il est possible d'attribuer à chaque élément de S l' une des deux couleurs différentes de sorte que dans chaque sous-ensemble A_i, il y a des éléments qui ont été assigné chaque couleur. Soit $m(d)$ le plus grand entier tel que chaque collection de moins de $m(d)$ fixe chaque con- La coloration des éléments d est bicolore.

a) Montrer que la collection de tous les sous-ensembles avec d éléments d'un ensemble S avec $2d - 1$ éléments n'est pas bicolore.

b) Montrez que $m(2) = 3$.

** **c)** Montrer que $m(3) = 7$. [*Astuce:* Montrer que la collection tion $\{1, 3, 5\}$, $\{1, 2, 6\}$, $\{1, 4, 7\}$, $\{2, 3, 4\}$, $\{2, 5, 7\}$, $\{3, 6, 7\}$, $\{4, 5, 6\}$ n'est pas bicolore. Montrez ensuite que toutes les collections de six ensembles de trois éléments sont 2 couleurs.]

35. Un professeur écrit 20 questions à choix multiples, chacune avec la réponse possible a, b, c ou d, pour un discret test de mathématiques. Si le nombre de questions avec a, b, c, et d comme leur réponse est 8, 3, 4 et 5, respectivement, comment de nombreuses réponses différentes sont possibles, si les questions peut être placé dans n'importe quel ordre?

36. Combien d'arrangements différents existe-t-il pour huit personnes assis à une table ronde, où deux arrangements sont considéré comme le même si l'un peut être obtenu de l'autre par une rotation?

37. De combien de façons existe-t-il d'affecter 24 élèves à cinq conseillers pédagogiques?

38. De combien de façons existe-t-il de choisir une douzaine de pommes boisseau contenant 20 pommes Delicious indiscernables, 20 pommes Macintosh indiscernables et 20 pommes indistinctes pommes Granny Smith, si au moins trois de chaque doit être choisi?

39. Combien de solutions existe-t-il pour l'équation $x_1 + x_2 + x_3 = 17$, où x_1, x_2 et x_3 sont des entiers non négatifs avec

a) $x_1 > 1$, $x_2 > 2$ et $x_3 > 3$?

b) $x_1 < 6$ et $x_3 > 5$?

c) $x_1 < 4$, $x_2 < 3$ et $x_3 > 5$?

40. a) Combien de chaînes différentes peuvent être faites à partir du mot *PEPPERCORN* lorsque toutes les lettres sont utilisées?

b) Combien de ces chaînes commencent et finissent par le lettre P ?

c) Dans combien de ces chaînes sont les trois lettres P s consécutif?

41. Combien de sous-ensembles d'un ensemble de dix éléments

a) a moins de cinq éléments?

b) a plus de sept éléments?

c) avoir un nombre impair d'éléments?

42. Un témoin d'un délit de fuite a déclaré à la police que la plaque d'immatriculation de la voiture dans l'accident, qui contient trois lettres suivies de trois chiffres, commence par la lettre teurs *AS* et contient à la fois les chiffres 1 et 2. Combien différentes plaques d'immatriculation peuvent correspondre à cette description?

43. De combien de façons existe-t-il de mettre n objets identiques m des conteneurs distincts pour qu'aucun conteneur ne soit vide?

44. Combien y a-t-il de façons de faire asseoir six garçons et huit filles dans une rangée de chaises de sorte qu'il n'y ait pas deux garçons assis à côté de L'une et l'autre?

45. Combien y a-t-il de façons de distribuer six objets à cinq boîtes si

a) les objets et les boîtes sont étiquetés?
b) les objets sont étiquetés, mais les boîtes ne sont pas étiquetées?
c) les objets ne sont pas étiquetés, mais les boîtes sont étiquetées?
d) les objets et les boîtes ne sont pas étiquetés?

46. De combien de façons existe-t-il de répartir cinq objets six cases si

a) les objets et les boîtes sont étiquetés?
b) les objets sont étiquetés, mais les boîtes ne sont pas étiquetées?
c) les objets ne sont pas étiquetés, mais les boîtes sont étiquetées?
d) les objets et les boîtes ne sont pas étiquetés?

Le **nombre de Stirling sans signe du premier type** $c(n, k)$, où k et n sont des entiers avec $1 \leq k \leq n$, est égal au nombre de façons d'organiser n personnes autour de k tables circulaires avec au au moins une personne assise à chaque table, où deux sièges *m les* gens autour d'une table circulaire sont considérés comme les mêmes si tout le monde a le même voisin de gauche et le même voisin de droite bor.

47. Trouvez ces nombres Stirling sans signe du premier type.

a) c (3,2) **b)** c (4,2)
c) c (4,3) **d)** c (5,4)

48. Montrer que si n est un entier positif, alors $\sum_{j=1}^{n} c(n, j) = n!$.

49. Montrer que si n est un entier positif avec $n \geq 3$, alors $c(n, n-2) = (3n-1)C(n, 3)/4$.

∗ **50.** Montrer que si n et k sont des entiers avec $1 \leq k < n$, alors $c(n+1, k) = c(n, k-1) + nc(n, k)$.

51. Donnez une preuve combinatoire que 2^n divise $n!$ chaque fois que n est un entier encore positif. [*Astuce:* utilisez le théorème 3 dans tion 6.5 pour compter le nombre de permutations de $2n$ objets où il y a deux objets indiscernables de n différences différents types.

52. Combien de séquences d'ARN à 11 éléments se composent de 4 As, 3C, 2U et 2G et se terminent par CAA?

Les exercices 53 et 54 sont basés sur une discussion dans [RoTe09]. Une méthode utilisée dans les années 1960 pour séquencer les chaînes d'ARN utilisées des enzymes pour briser les chaînes après certains maillons. Certaines enzymes briser les chaînes d'ARN après chaque lien G, tandis que d'autres les brisent après chaque lien C ou U. En utilisant ces enzymes, il est parfois possible de séquencer correctement toutes les bases d'une chaîne d'ARN.

∗ **53.** Supposons que lorsqu'une enzyme qui rompt les chaînes d'ARN après ter chaque maillon G est appliqué à une chaîne de 12 maillons, les fragments obtenus sont G, CCG, AAAG et UCCG, et lorsqu'un enzyme qui rompt les chaînes d'ARN après chaque liaison C ou U est appliqué, les fragments obtenus sont C, C, C, C, GGU, et GAAAG. Pouvez-vous déterminer l'ensemble de l'ARN à 12 liaisons chaîne à partir de ces deux ensembles de fragments? Si oui, qu'est-ce que c'est Chaîne d'ARN?

∗ **54.** Supposons que lorsqu'une enzyme qui rompt les chaînes d'ARN après ter chaque maillon G est appliqué à une chaîne de 12 maillons, les fragments obtenus sont AC, UG et ACG et lorsqu'une enzyme qui rompt les chaînes d'ARN après l'application de chaque liaison C ou U, les fragments obtenus sont U, GAC et GAC. Peut tu déterminer la chaîne d'ARN entière de ces deux ensembles de des fragments? Si oui, quelle est cette chaîne d'ARN?

55. Concevoir un algorithme pour générer toutes les r- permutations d'un ensemble fini lorsque la répétition est autorisée.

56. Concevoir un algorithme pour générer toutes les combinaisons R d'un ensemble fini lorsque la répétition est autorisée.

∗ **57.** Montrer que si m et n sont des entiers avec $m \geq 3$ et $n \geq 3$, alors $R(m, n) \leq R(m, n-1) + R(m-1, n)$.

∗ **58.** Montrer que $R(3, 4) \geq 7$ en montrant que dans un groupe de six les gens, où deux personnes sont des amis ou des ennemis, il ne sont pas nécessairement trois amis mutuels ou quatre emies.

Projets informatiques

Écrivez des programmes avec ces entrées et sorties.

1. Étant donné un entier positif n et un entier non négatif non dépassant n, trouver le nombre de r- permutations et r - combinaisons d'un ensemble avec n éléments.

2. Étant donné les entiers positifs n et r, trouvez le nombre de r -permutations lorsque la répétition est autorisée et r -combinaisons lorsque la répétition est autorisée d'un ensemble avec n elements.

3. Étant donné une séquence d'entiers positifs, trouvez le plus long plissement et la plus longue sous-séquence décroissante de la séquence.

∗ **4.** Étant donné une équation $x_1 + x_2 + \cdots + x_n = C$, où C est un constante, et $x_1, x_2, \ldots, x_n$ sont des entiers non négatifs, liste toutes les solutions.

5. Étant donné un entier positif n, énumérez toutes les permutations du mettre $\{1, 2, 3, \ldots, n\}$ dans l'ordre lexicographique.

6. Étant donné un entier positif n et un entier non négatif r n'excédant pas n, énumérer toutes les combinaisons r de l'ensemble $\{1, 2, 3, \ldots, n\}$ dans l'ordre lexicographique.

7. Étant donné un entier positif n et un entier non négatif r ne dépassant pas n, énumérer toutes les r- permutations de l'ensemble $\{1, 2, 3, \ldots, n\}$ dans l'ordre lexicographique.

8. Étant donné un entier positif n, énumérez toutes les combinaisons des définir $\{1, 2, 3, \ldots, n\}$.

9. Étant donné les entiers positifs n et r, énumérer toutes les r- permutations, avec répétition autorisée, de l'ensemble $\{1, 2, 3, \ldots, n\}$.

10. Étant donné les entiers positifs n et r, énumérer toutes les combinaisons r, avec répétition autorisée, de l'ensemble $\{1, 2, 3, \ldots, n\}$.

Calculs et explorations

Utilisez un ou plusieurs programmes informatiques que vous avez écrits pour effectuer ces exercices.

1. Trouvez le nombre de résultats possibles dans un jeu à deux équipes off lorsque le vainqueur est la première équipe à gagner 5 sur 9, 6 sur 11, 7 sur 13 et 8 sur 15.

2. Quels coefficients binomiaux sont impairs? Pouvez-vous formuler un conjecture basée sur des preuves numériques?

3. Vérifier que $C(2n, n)$ est divisible par le carré d'un nombre premier, lorsque $n = 1, 2$, ou 4, pour autant de nombres entiers positifs n que vous pouvez. [Le théorème qui dit que $C(2n, n)$ est divisible par le carré d'un nombre premier avec $n = 1, 2$, ou 4 a été prouvé en 1996 par Andrew Granville et Olivier Ramaré. Leur la preuve a réglé une conjecture faite en 1980 par Paul Erd˝os et Ron Graham.]

4. Trouvez autant d'entiers impairs n inférieurs à 200 que vous le pouvez pour qui $C(n, \lfloor n/2 \rfloor)$ ne sont pas divisible par le carré d'un nombre premier. Formulez une conjecture basée sur vos preuves.

∗ **5.** Pour chaque entier inférieur à 100, déterminez si $C(2n, n)$ est divisible par 3. Pouvez-vous formuler une conjecture qui raconte us pour quels entiers n le coefficient binomial $C(2n, n)$ est divisible par 3 sur la base des chiffres de la base trois expansion de n ?

6. Générez toutes les permutations d'un ensemble à huit éléments.

7. Générez toutes les 6 permutations d'un ensemble de neuf éléments.

8. Générez toutes les combinaisons d'un ensemble avec huit éléments.

9. Générez toutes les 5 combinaisons avec répétition autorisée d'un sertie de sept éléments.

Projets d'écriture

Répondez à ces questions par des essais en utilisant des sources extérieures.

1. Décrivez quelques-unes des premières utilisations du principe de Dirichlet et d'autres mathématiciens.

2. Discuter des façons dont la numérotation téléphonique actuelle le plan peut être étendu pour répondre à la demande rapide pour plus de numéros de téléphone. (Voyez si vous pouvez en trouver des propositions émanant du secteur des télécommunications secteur.) Pour chaque nouveau plan de numérotation dont vous discutez, comment trouver le nombre de numéros de téléphone différents, il les soutiens.

3. Discuter de l'importance du raisonnement combinatoire dans le gène séquençage et problèmes connexes impliquant des génomes.

4. De nombreuses identités combinatoires sont décrites dans ce livre. Trouvez quelques sources de telles identités et décrivez les identités combinatoires en plus de celles déjà introduites dans ce livre. Donnez des preuves représentatives, y compris combinatoires, de certaines de ces identités.

5. Décrivez les différents modèles utilisés pour modéliser répartition des particules en mécanique statistique, y compris Maxwell – Boltzmann, Bose – Einstein et Fermi – Dirac statistiques. Dans chaque cas, décrivez les techniques de comptage utilisé dans le modèle.

6. Définissez les nombres de Stirling du premier type et décrivez certaines de leurs propriétés et les identités qu'ils satisfont.

7. Décrivez quelques-unes des propriétés et des identités les nombres linguistiques du deuxième type satisfont, y nection entre les nombres de Stirling du premier et du second sortes.

8. Décrire les dernières découvertes de valeurs et de limites pour Numéros de Ramsey.

9. Décrire des moyens supplémentaires de générer toutes les permutations d'un ensemble avec n éléments en plus de ceux trouvés dans la section 6.6. Comparez ces algorithmes et les algorithmes décrits dans le texte et les exercices de la section 6.6 en termes de leur complexité informatique.

10. Décrivez au moins une façon de générer toutes les partitions de un entier positif n . (Voir l'exercice 47 à la section 5.3.)

Probabilité discrète

La combinatoire et la théorie des probabilités ont des origines communes. La théorie de la probabilité était développé pour la première fois il y a plus de 300 ans, lorsque certains jeux de hasard ont été analysés. Bien que la théorie des probabilités ait été à l'origine inventée pour étudier le jeu, elle joue maintenant un rôle essentiel rôle dans une grande variété de disciplines. Par exemple, la théorie des probabilités est largement appliquée dans l'étude de la génétique, où elle peut être utilisée pour aider à comprendre l'hérédité des traits. Bien sûr, la probabilité reste une partie extrêmement populaire des mathématiques en raison de son applicabilité au jeu, qui continue d'être une entreprise humaine extrêmement populaire.

En informatique, la théorie des probabilités joue un rôle important dans l'étude de la plexité des algorithmes. En particulier, les idées et les techniques de la théorie des probabilités sont utilisées pour déterminer la complexité moyenne des cas des algorithmes. Des algorithmes probabilistes peuvent être utilisés pour résoudre de nombreux problèmes qui ne peuvent pas être résolus facilement ou pratiquement par des algorithmes déterministes. Dans un algorithme probabiliste, au lieu de toujours suivre les mêmes étapes quand on leur donne le même entrée, comme le fait un algorithme déterministe, l'algorithme fait un ou plusieurs choix aléatoires, ce qui peut conduire à une sortie différente. En combinatoire, la théorie des probabilités peut même être utilisée pour montrent qu'il existe des objets avec certaines propriétés. La méthode probabiliste, une technique en com- binatorics introduite par Paul Erd˝os et Alfréd Rényi, montre qu'un objet avec un existe en montrant qu'il existe une probabilité positive qu'un objet construit de façon aléatoire a cette propriété. La théorie des probabilités peut nous aider à répondre à des questions qui comportent de l'incertitude, comme comme déterminant si nous devons rejeter un message électronique entrant comme spam sur la base des mots qui apparaissent dans le message.

Une introduction à la probabilité discrète

introduction

La théorie des probabilités remonte à 1526 lorsque le mathématicien, médecin et joueur italien Girolamo Cardano a écrit le premier traitement systématique connu du sujet dans son livre *Liber de Ludo Aleae* (*Livre sur les jeux de hasard*). (Ce livre n'a été publié qu'en 1663, ce qui peut avoir freiné le développement de la théorie des probabilités.) Au XVIIe siècle, Le mathématicien français Blaise Pascal a déterminé les chances de gagner des paris populaires en fonction sur le résultat lorsqu'une paire de dés est lancée à plusieurs reprises. Au XVIIIe siècle, les Français mathématicien Laplace, qui a également étudié le jeu, a défini la probabilité d'un événement comme nombre de résultats positifs divisé par le nombre de résultats possibles. Par exemple, le probabilité qu'un dé monte un nombre impair quand il est lancé est le nombre de succès résultats - à savoir, le nombre de façons dont il peut arriver impair - divisé par le nombre de possibles résultats, à savoir le nombre de façons différentes dont le dé peut surgir. Il y a un total de six résultats possibles , à savoir, 1 , 2 , 3 , 4 , 5 , et 6 et exactement trois d' entre elles sont réussies résultats, à savoir 1, 3 et 5. Par conséquent, la probabilité que le dé monte un nombre impair est 3 / 6 = 1 / 2. (Notez qu'il a supposé que tous les résultats possibles sont également probables, ou, en d'autres termes, que le dé est juste.)

Dans cette section, nous nous limiterons aux expériences qui ont un nombre fini, tout aussi probable, résultats. Cela nous permet d'utiliser la définition de Laplace de la probabilité d'un événement. Nous allons continuer notre étude de probabilité dans la section 7.2, où nous étudierons des expériences avec de nombreux résultats qui ne sont pas nécessairement aussi probables. Dans la section 7.2, nous présenterons également

certains concepts clés de la théorie des probabilités, y compris la probabilité conditionnelle, l'indépendance événements et variables aléatoires. Dans la section 7.4, nous présenterons les concepts de l'attente et variance d'une variable aléatoire.

Probabilité finie

Une **expérience** est une procédure qui donne l'un d'un ensemble donné de résultats possibles. L' **échantillon l'espace** de l'expérience est l'ensemble des résultats possibles. Un **événement** est un sous-ensemble de l'échantillon espace. Définition de Laplace de la probabilité d'un événement avec un nombre fini de résultats possibles va maintenant être indiqué.

DÉFINITION 1 Si S est un espace échantillon non vide fini de résultats également probables, et E est un événement, cela

$| E |$

est, un sous-ensemble de S, alors la *probabilité* de E est $p(E) = \quad |S|$.

La probabilité d'un l'événement ne peut jamais être négatif ou supérieur à un!

Selon la définition de Laplace, la probabilité d'un événement est comprise entre 0 et 1. Pour voir cela, notons que si E est un événement d'un espace d'échantillon fini S, alors $0 \leq |E| \leq |S|$, parce que $E \subseteq S$. Ainsi, $0 \leq p(E) = |E| / |S| \leq 1$.

Les exemples 1 à 7 illustrent comment la probabilité d'un événement est trouvée.

EXEMPLE 1 Une urne contient quatre boules bleues et cinq boules rouges.Quelle est la probabilité qu'une balle choisie à aléatoire de l'urne est bleu?

Solution: pour calculer la probabilité, notez qu'il y a neuf résultats possibles et quatre de ces résultats possibles produisent une boule bleue. Par conséquent, la probabilité qu'une balle bleue soit choisie est égal à $4/9$. ▲

EXEMPLE 2 Quelle est la probabilité que lorsque deux dés sont lancés, la somme des nombres sur les deux dés est 7?

Solution: Il y a un total de 36 résultats possibles tout aussi probables lorsque deux dés sont lancés. (La règle du produit peut être utilisée pour voir ceci; parce que chaque dé a six résultats possibles, le total

GIROLAMO CARDANO (1501-1576) Cardano, né à Pavie, en Italie, était l'enfant illégitime de Fazio Cardano, avocat, mathématicien et ami de Léonard de Vinci, et Chiara Micheria, une jeune veuve. Malgré la maladie et la pauvreté, Cardano a pu étudier dans les universités de Pavie et Padoue, d'où il a obtenu son diplôme de médecine. Cardano n'a pas été accepté au Collège des médecins de Milan en raison de son naissance illégitime, ainsi que son excentricité et son style de confrontation. Néanmoins, ses compétences médicales étaient très apprécié. L'une de ses principales réalisations en tant que médecin est la première description de la fièvre typhoïde.

Cardano a publié plus de 100 livres sur un large éventail de sujets, y compris la médecine, le naturel sciences, mathématiques, jeux d'argent, inventions et expériences physiques et astrologie. Il a également écrit un fascinant autobiographie. En mathématiques, le livre de Cardano *Ars Magna*, publié en 1545, a jeté les bases de algèbre abstraite. C'était le livre le plus complet sur l'algèbre abstraite depuis plus d'un siècle; il présente de nombreuses idées nouvelles de Cardano et d'autres, y compris des méthodes pour résoudre des équations cubiques et quartiques à partir de leurs coefficients. Cardano a également réalisé plusieurs contributions importantes à la cryptographie. Cardano était un défenseur de l'éducation pour les sourds, croyant, contrairement à ses contemporains, que les personnes sourdes pouvaient apprendre à lire et à écrire avant d'apprendre à parler, et pouvaient utiliser leur esprit aussi bien qu'entendre les gens.

Cardano manquait souvent d'argent. Cependant, il s'est maintenu solvable en jouant et en gagnant de l'argent en battant les autres aux échecs. Son livre sur les jeux de hasard, *Liber de Ludo Aleae*, écrit en 1526 (mais publié en 1663), offre la première systématique traitement des probabilités; il décrit également des moyens efficaces de tricher. Cardano était considéré comme un homme de caractère moral douteux; il était souvent décrit comme un menteur, un joueur, un lecher et un hérétique.

nombre de résultats lorsque deux dés sont lancés est $6^2 = 36$.) Il y a six résultats réussis, à savoir, $(1, 6)$, $(2, 5)$, $(3, 4)$, $(4, 3)$, $(5, 2)$ et $(6, 1)$, où les valeurs des première et deuxième les dés sont représentés par une paire ordonnée. Par conséquent, la probabilité qu'un sept apparaisse lorsque deux dés justes sont laminées est de $6/36 = 1/6$. ▲

Les loteries sont extrêmement populaires dans le monde. Nous pouvons facilement calculer les chances de gagner différents types de loteries, comme illustré dans les exemples 3 et 4. (L'étrange de gagner le les loteries populaires Mega Millions et Powerball sont étudiées dans les exercices supplémentaires.)

EXEMPLE 3 Dans une loterie, les joueurs gagnent un gros lot en choisissant quatre chiffres qui correspondent, dans le bon ordre, quatre chiffres sélectionnés par un processus mécanique aléatoire. Un plus petit prix est gagné si seulement trois chiffres sont appariés. Quelle est la probabilité qu'un joueur remporte le gros lot? Quelle est la probabilité qu'un joueur gagne le petit prix?

Solution: Il n'y a qu'une seule façon de choisir correctement les quatre chiffres. Par la règle du produit, il sont $10^4 = 10,000$ façons de choisir quatre chiffres. Par conséquent, la probabilité qu'un joueur remporte le grand prix est de $1 /$ dix $, 000 = 0.0001$.

Les joueurs gagnent le plus petit prix lorsqu'ils choisissent correctement exactement trois des quatre chiffres. Exactement un chiffre doit être faux pour obtenir trois chiffres corrects, mais pas tous les quatre corrects. Par la somme règle, pour trouver le nombre de façons de choisir exactement trois chiffres correctement, nous ajoutons le nombre de façons de choisir quatre chiffres correspondant aux chiffres choisis dans toutes sauf la i ème position, pour $i = 1, 2, 3, 4$.

Pour compter le nombre de succès avec le premier chiffre incorrect, notez qu'il y a neuf choix possibles pour le premier chiffre (tous sauf le bon chiffre) et un choix pour chacun des d'autres chiffres, à savoir les chiffres corrects pour ces emplacements. Par conséquent, il y a neuf façons de choisir quatre chiffres où le premier chiffre est incorrect, mais les trois derniers sont corrects. De même, il y a neuf façons de choisir quatre chiffres où le deuxième chiffre est incorrect, neuf avec le troisième chiffre incorrect, et neuf avec le quatrième chiffre incorrect. Par conséquent, il y a un total de 36 façons de choisir quatre chiffres avec exactement trois des quatre chiffres corrects. Ainsi, la probabilité qu'un joueur gagne le plus petit prix est de $36/10,000 = 9/$2,5 mille $= 0.0036$. ▲

EXEMPLE 4 Il existe maintenant de nombreuses loteries qui accordent des prix énormes aux personnes qui choisissent correctement un ensemble de six nombres sur les n premiers entiers positifs, où n est généralement compris entre 30 et 60. Ce est la probabilité qu'une personne choisisse les six bons nombres sur 40?

Solution: Il n'y a qu'une seule combinaison gagnante. Le nombre total de façons de choisir six un nombre sur 40 est

$$C(40, 6) = \frac{40!}{34!\,6!} = 3,838,380.$$

Par conséquent, la probabilité de choisir une combinaison gagnante est del $/ 3,838,380 \approx 0.00000026$. (Ici, le symbole ≈ signifie approximativement égal à.) ▲

PIERRE-SIMON LAPLACE (1749–1827) Pierre-Simon Laplace est issu de modestes origines normandes. Dans son enfance, il a fait ses études dans une école dirigée par les Bénédictins. A 16 ans il entre à l'Université de Caen l'intention d'étudier la théologie. Cependant, il s'est vite rendu compte que ses véritables intérêts étaient les mathématiques. Après avoir complété ses études, il a été nommé professeur provisoire à Caen, et en 1769, il est devenu professeur de mathématiques à l'École militaire de Paris.

Laplace est surtout connu pour ses contributions à la mécanique céleste, à l'étude des mouvements du corps céleste. ies. Son *Traité de Mécanique Céleste* est considéré comme l'un des plus grands travaux scientifiques du début du XIXe siècle. tury. Laplace a été l'un des fondateurs de la théorie des probabilités et a apporté de nombreuses contributions à la statistique mathématique. tics. Son travail dans ce domaine est documenté dans son livre *Théorie Analytique des Probabilités* , dans lequel il définit la probabilité d'un événement comme le rapport du nombre de résultats favorables au nombre total de résultats d'une expérience.

Laplace était célèbre pour sa flexibilité politique. Il était fidèle, successivement, à la République française, à Napoléon et au roi Louis XVIII. Cette flexibilité lui a permis d'être productif avant, pendant et après la Révolution française.

Le poker et d'autres jeux de cartes gagnent en popularité. Pour gagner à ces jeux, il est utile de connaître la probabilité de mains différentes. Nous pouvons trouver la probabilité de mains spécifiques qui se posent dans les jeux de cartes en utilisant les techniques développées jusqu'à présent. Un jeu de cartes contient 52 cartes. Là sont 13 différents types de cartes, avec quatre cartes de chaque type. (Parmi les termes couramment utilisés au lieu de «genre» sont «rang», «valeur nominale», «dénomination» et «valeur».) Ces types sont deux, trois, quatre, cinq, six, sept, huit, neuf, des dizaines, des crics, des reines, des rois et des asIl y a également quatre costumes: pique, massues, coeurs et diamants, chacun contenant 13 cartes, avec une carte de chaque type dans un costume. Dans de nombreux jeux de poker, une main se compose de cinq cartes.

EXEMPLE 5 Trouvez la probabilité qu'une main de cinq cartes au poker contienne quatre cartes d'un même type.

Solution: selon la règle du produit, le nombre de mains de cinq cartes avec quatre cartes d'un même type est le produit du nombre de façons de choisir un type, du nombre de façons de choisir les quatre ce type sur les quatre dans le jeu de ce type, et le nombre de façons de choisir la cinquième carte. C'est

$$C(13, 1)\, C(4, 4)\, C(48, 1).$$

Dans l'exemple 11 de la section 6.3, il y a $C(52, 5)$ mains différentes de cinq cartes. D'où le la probabilité qu'une main contienne quatre cartes d'un même type est

$$\frac{C(13, 1)\, C(4, 4)\, C(48, 1)}{C(52, 5)} = \frac{13 \cdot 1 \cdot 48}{2,598,960} \approx 0.00024.$$ ▲

EXEMPLE 6 Quelle est la probabilité qu'une main de poker contienne un full, c'est-à-dire trois d'un même type et deux d'un autre genre?

Solution: selon la règle du produit, le nombre de mains contenant une maison pleine est le produit du nombre de façons de choisir deux types dans l'ordre, le nombre de façons de choisir trois sur quatre pour le premier type et le nombre de façons d'en choisir deux sur quatre pour le second(Notez que l'ordre des deux types compte, parce que, par exemple, trois reines et deux as sont différents de trois as et deux reines.) Nous voyons que le nombre de mains contenant une maison pleine est

$$P(13, 2)\, C(4, 3)\, C(4, 2) = 13 \cdot 12 \cdot 4 \cdot 6 = 3744.$$

Parce qu'il y a $C(52, 5) = 2,598,960$ mains de poker, la probabilité d'un full est

$$\frac{3744}{2,598,960} \approx 0.0014.$$ ▲

EXEMPLE 7 Quelle est la probabilité que les nombres 11, 4, 17, 39 et 23 soient tirés dans cet ordre à partir d'un bac contenant 50 billes étiquetées avec les chiffres $1, 2, \ldots, 50$ si (a) la balle sélectionnée n'est pas retournée dans le bac avant que la balle suivante ne soit sélectionnée et (b) la balle sélectionnée est retournée dans le bac avant la balle suivante est sélectionnée?

Solution: (a) Selon la règle du produit, il existe 50 · 49 · 48 · 47 · 46 = 254 251 , 200 façons de sélectionner les balles parce qu'à chaque fois qu'une balle est tirée, il y a une balle de moins à choisirPar conséquent, la probabilité que 11, 4, 17, 39 et 23 sont tirées dans cet ordre est del ⁄ 254 , 251 , 200. Ceci est un exemple d' **échantillonnage sans remplacement** .

(b) Selon la règle du produit, il y a 50^5 = 312 , 500 , 000 façons de sélectionner les boules car il y a 50 balles possibles au choix à chaque fois qu'une balle est tirée.Par conséquent, la probabilité que 11, 4, 17, 39 et 23 sont tirées dans cet ordre est del ⁄ 312 , 500 , 000. Ceci est un exemple d' **échantillonnage avec remplacement** . ▲

Probabilités de compléments et d'unions d'événements

Nous pouvons utiliser des techniques de comptage pour trouver la probabilité d'événements dérivés d'autres événements.

THÉORÈME 1 Que E soit un événement dans un espace échantillon S . La probabilité de l'événement $E = S - E$, le complément événement mentaire de E , est donné par

$$p(E) = 1 - p(E).$$

Preuve: Pour trouver la probabilité de l'événement $E = S - E$, notez que $|E| = |S| - |E|$. Par conséquent,

$$p(E) = \frac{|S| - |E|}{|S|} = 1 - \frac{|E|}{|S|} = 1 - p(E).$$

Il existe une stratégie alternative pour trouver la probabilité d'un événement lorsqu'une approche directe ne fonctionne pas bien. Au lieu de déterminer la probabilité de l'événement, la probabilité de son complément peut être trouvé.C'est souvent plus facile à faire, comme le montre l'exemple 8.

EXEMPLE 8 Une séquence de 10 bits est générée aléatoirement.Quelle est la probabilité qu'au moins un de ces bits est 0?

Solution: Soit E l'événement au moins un des 10 bits égal à 0. Alors E est l'événement selon lequel tous les les bits sont 1s. Parce que l'espace d'échantillonnage S est l'ensemble de toutes les chaînes de bits de longueur 10, il s'ensuit que

$$p(E) = 1 - p(E) = 1 - \frac{|E|}{|S|} = 1 - \frac{1}{2^{10}}$$

$$= 1 - \frac{1}{1024} = \frac{1023}{1024}.$$

Par conséquent, la probabilité que la chaîne de bits contiendra au moins un bit 0 est 1023⁄ 1024. Il est tout à fait difficile de trouver cette probabilité directement sans utiliser le théorème 1. ▲

Nous pouvons également trouver la probabilité de l'union de deux événements.

THÉORÈME 2 Laissez E_1 et E_2 soit des événements dans l'espace échantillon S . alors

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2).$$

Preuve: Utilisation de la formule donnée à la section 2.2 pour le nombre d'éléments dans l'union de deux ensembles, il s'ensuit que

$$|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|.$$

Par conséquent,

$$p(E_1 \cup E_2) = \frac{|E_1 \cup E_2|}{|S|}$$
$$= \frac{|E_1| + |E_2| - |E_1 \cap E_2|}{|S|}$$
$$= \frac{|E_1|}{|S|} + \frac{|E_2|}{|S|} - \frac{|E_1 \cap E_2|}{|S|}$$
$$= p(E_1) + p(E_2) - p(E_1 \cap E_2).$$

EXEMPLE 9 Quelle est la probabilité qu'un entier positif sélectionné au hasard dans l'ensemble des entiers positifs n'excédant pas 100 est divisible par 2 ou 5?

Solution: Soit E_1 l'événement où l'entier sélectionné au hasard est divisible par 2, et soit E_2 soit l'événement qu'il est divisible par 5. Alors $E_1 \cup E_2$ est l'événement qu'il est divisible par 2 ou 5. De plus, $E_1 \cap E_2$ est l'événement qu'il est divisible par 2 et 5, ou de manière équivalente, qu'il est divisible par 10. Parce que $|E_1| = 50$, $|E_2| = 20$, et $|E_1 \cap E_2| = 10$, il s'ensuit que

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$
$$= \frac{50}{100} + \frac{20}{100} - \frac{\text{dix}}{100} = \frac{3}{5}.$$

▲

Raisonnement probabiliste

Un problème courant consiste à déterminer lequel des deux événements est le plus probable. Analyser la probabilité Les événements de ce type peuvent être délicats. L'exemple 10 décrit un problème de ce type. Il discute d'un célèbre problème provenant du jeu télévisé *Let's Make a Deal* et nommé d'après l'hôte de l'émission, Monty Hall.

EXEMPLE 10 **Le casse-tête à trois portes de Monty Hall** Supposons que vous participiez à un jeu télévisé. Tu as un chance de gagner un grand prix. Vous êtes invité à sélectionner l'une des trois portes à ouvrir; le gros lot est derrière l'une des trois portes et les deux autres portes sont perdantes. Une fois que vous avez sélectionné une porte, l'hôte du jeu télévisé, qui sait ce qui se trouve derrière chaque porte, fait ce qui suit. Premièrement, que ce soit ou non vous avez sélectionné la porte gagnante, il ouvre l'une des deux autres portes qu'il sait être perdante porte (sélection au hasard si les deux perdent des portes). Il vous demande ensuite si vous souhaitez passer les portes. Quelle stratégie devez-vous utiliser? Si vous changez de porte ou conservez votre original sélection, ou n'a-t-il pas d'importance?

Solution: la probabilité que vous sélectionniez la bonne porte (avant que l'hôte n'ouvre une porte et ne vous demande si vous voulez changer) est de $1/3$, parce que les trois portes sont également susceptibles d'être la bonne porte. La probabilité que ce soit la bonne porte ne change pas une fois que l'hôte du jeu télévisé ouvre l'une des autres portes, car il ouvrira toujours une porte que le prix n'est pas derrière.

La probabilité que vous ayez mal sélectionné est la probabilité que le prix soit derrière l'un des deux portes que vous n'avez pas sélectionnées. Par conséquent, la probabilité que vous avez sélectionné est incorrectement $2/3$. Si vous avez mal choisi, lorsque l'hôte du jeu télévisé ouvre une porte pour vous montrer que le prix est pas derrière, le prix est derrière l'autre porte. Vous gagnerez toujours si votre choix initial était incorrect et vous changez de portes. Ainsi, par des portes changeantes, la probabilité que vous gagnez est $2/3$. Dans d' autres En d'autres termes, vous devez toujours changer de porte lorsque l'hôte du jeu vous en donne la possibilité. Cela double la probabilité de gagner. (Un traitement plus rigoureux de ce puzzle peut être que l'on trouve dans l'exercice 15 de la section 7.3. Pour bien plus sur ce fameux puzzle et ses variations, voir [Ro09].)

▲

Des exercices

1. Quelle est la probabilité qu'une carte sélectionnée au hasard à partir d'un jeu standard de 52 cartes est un as?

2. Quelle est la probabilité qu'un dé équitable arrive à six lorsque c'est roulé?

3. Quelle est la probabilité qu'un entier choisi au hasard choisi parmi les 100 premiers entiers positifs est impair?

4. Quelle est la probabilité qu'un jour choisi au hasard année bissextile (avec 366 jours possibles) est en avril?

5. Quelle est la probabilité que la somme des nombres sur deux dés est égal quand ils sont lancés?

6. Quelle est la probabilité qu'une carte choisie au hasard à partir d'un jeu standard de 52 cartes est un as ou un coeur?

7. Quelle est la probabilité que lorsqu'une pièce est retournée six fois de suite, ça atterrit tête en tête à chaque fois?

8. Quelle est la probabilité qu'une main de poker à cinq cartes tains l'as de cœur?

9. Quelle est la probabilité qu'une main de poker à cinq cartes ne contient pas la reine de cœur?

10. Quelle est la probabilité qu'une main de poker à cinq cartes tains les deux de diamants et les trois de pique?

11. Quelle est la probabilité qu'une main de poker à cinq cartes contient les deux de diamants, les trois de pique, les six de coeurs, les dix clubs et le roi des coeurs?

12. Quelle est la probabilité qu'une main de poker à cinq cartes contient exactement un as?

13. Quelle est la probabilité qu'une main de poker à cinq cartes contient au moins un as?

14. Quelle est la probabilité qu'une main de poker à cinq cartes tains cartes de cinq types différents?

15. Quelle est la probabilité qu'une main de poker à cinq cartes contient deux paires (c'est-à-dire deux de chacun des deux types différents et une cinquième carte d'un troisième type)?

16. Quelle est la probabilité qu'une main de poker à cinq cartes contient une couleur, c'est-à-dire cinq cartes de la même couleur?

17. Quelle est la probabilité qu'une main de poker à cinq cartes contient une ligne droite, c'est-à-dire cinq cartes qui ont consécutives sortes? (Notez qu'un as peut être considéré soit comme le la plus haute carte d'une ligne droite A-2-3-4-5 ou la plus haute 10-JQKA droit.)

18. Quelle est la probabilité qu'une main de poker à cinq cartes contient une quinte flush, c'est-à-dire cinq cartes de la même couleur types consécutifs?

∗ **19.** Quelle est la probabilité qu'une main de poker à cinq cartes contient des cartes de cinq types différents et ne contient pas de flush ou une ligne droite?

20. Quelle est la probabilité qu'une main de poker à cinq cartes contient une quinte flush royale, c'est-à-dire le 10, jack, queen, king et as d'un costume?

21. Quelle est la probabilité qu'une mort équitable ne survienne nombre pair quand il est roulé six fois?

22. Quelle est la probabilité qu'un entier positif ne dépasse pas 100 sélectionnés au hasard est divisible par 3?

23. Quelle est la probabilité qu'un entier positif ne dépasse pas 100 sélectionnés au hasard est divisible par 5 ou 7?

24. Trouvez la probabilité de gagner à une loterie en sélectionnant le corriger six entiers, où l'ordre dans lequel ces entiers sont sélectionnés, peu importe, à partir de l'intégra-gers ne dépassant pas

a) 30. **b)** 36. **c)** 42. **d)** 48.

25. Trouvez la probabilité de gagner à une loterie en sélectionnant le corriger six entiers, où l'ordre dans lequel ces entiers sont sélectionnés, peu importe, à partir de l'intégra-gers ne dépassant pas

a) 50. **b)** 52. **c)** 56. **d)** 60.

26. Trouvez la probabilité de ne sélectionner aucun des six bons tegers dans une loterie, où l'ordre dans lequel ces entiers sont sélectionnés n'a pas d'importance, parmi les entiers positifs non dépassement

a) 40. **b)** 48. **c)** 56. **d)** 64.

27. Trouver la probabilité de sélectionner exactement l'un des bons six entiers dans une loterie, où l'ordre dans lequel ces les entiers sont sélectionnés n'a pas d'importance, du positif nombres entiers ne dépassant pas

a) 40. **b)** 48. **c)** 56. **d)** 64.

28. Dans une superloterie, un joueur sélectionne 7 numéros parmi les 80 premiers entiers positifs. Quelle est la probabilité qu'un personne gagne le grand prix en choisissant 7 numéros qui figurent parmi les 11 numéros sélectionnés au hasard par un ordinateur.

29. Dans une superloterie, les joueurs gagnent une fortune s'ils choisissent huit nombres sélectionnés par un ordinateur parmi les positifs entiers ne dépassant pas 100. Quelle est la probabilité qu'un joueur gagne cette superloterie?

30. Quelle est la probabilité qu'un joueur d'une loterie gagne le prix offert pour avoir choisi correctement cinq (mais pas six) nombres sur six entiers choisis au hasard dans le entiers compris entre 1 et 40, inclus?

31. Supposons que 100 personnes participent à un concours et que différentes les gagnants sont sélectionnés au hasard pour les premier, deuxième et troisième prix. Quelle est la probabilité que Michelle gagne l'un des ces prix si elle fait partie des candidats?

32. Supposons que 100 personnes participent à un concours et que différentes les gagnants sont sélectionnés au hasard pour les premier, deuxième et troisième prix. Quelle est la probabilité que Kumar, Janice et Pedro chacun gagne un prix si chacun a participé au concours?

33. Quelle est la probabilité que Abby, Barry et Sylvia gagnent premier, deuxième et troisième prix, respectivement, par tirage au sort si 200 personnes participent à un concours et

a) personne ne peut gagner plus d'un prix.
b) gagner plus d'un prix est autorisé.

34. Quelle est la probabilité que Bo, Colleen, Jeff et Rohini gagner les premier, deuxième, troisième et quatrième prix, respectivement, dans un dessin si 50 personnes participent à un concours et

a) personne ne peut gagner plus d'un prix.
b) gagner plus d'un prix est autorisé.

35. À la roulette, une roue à 38 chiffres est tournée. De ce nombre, 18 sont rouges et 18 sont noirs. Les deux autres chiffres, qui ne sont ni noir ni rouge, sont 0 et 00. La probabilité que lorsque la roue tourne, elle atterrit sur un point particulier nombre est égal à $1/38$.

a) Quelle est la probabilité que la roue tombe sur un rouge nombre?

b) Quelle est la probabilité que la roue tombe sur un noir numéro deux fois de suite?

c) Quelle est la probabilité que la roue atterrisse sur 0 ou 00?

d) Quelle est la probabilité qu'en cinq tours la roue atterrit jamais sur 0 ou 00?

e) Quelle est la probabilité que la roue se pose sur l'un des les six premiers nombres entiers sur un tour, mais ne se pose pas sur l'un d'eux lors de la prochaine rotation?

36. Ce qui est plus probable: lancer un total de 8 lorsque deux dés sont lancés ou roulent un total de 8 lorsque trois dés sont lancés?

37. Ce qui est plus probable: lancer un total de 9 lorsque deux dés sont lancés ou roulent un total de 9 lorsque trois dés sont lancés?

38. Deux événements E_1 et E_2 sont appelés **indépendants** si $p(E_1 \cap E_2) = p(E_1)\, p(E_2)$. Pour chacun des éléments suivants paires d'événements, qui sont des sous-ensembles de l'ensemble de résultats bleus quand une pièce est lancée trois fois, déterminez qu'ils soient indépendants ou non.

a) E_1 : la queue arrive avec la pièce est lancée le premier temps; E_2 : les têtes se lèvent lorsque la pièce est lancée deuxième fois.

b) E_1 : la première pièce sort pile; E_2 : deux, et non trois, les têtes se relèvent.

c) E_1 : la deuxième pièce monte en queue; E_2 : deux, et non trois, les têtes se relèvent.

(Nous étudierons plus en détail l'indépendance des événements dans Section 7.2.)

39. Expliquez ce qui ne va pas avec la déclaration selon laquelle Monty Hall Three-Door Puzzle la probabilité que le prix est derrière la première porte que vous sélectionnez et la probabilité que le prix est derrière l'autre des deux portes qui Monty n'a pas ouvert sont à $1/2$, parce qu'il ya deux portes à gauche.

40. Supposons qu'au lieu de trois portes, il y ait quatre portes dans le puzzle de Monty Hall. Quelle est la probabilité que vous gagner en ne changeant pas une fois l'hôte, qui sait ce qui est derrière chaque porte, ouvre une porte perdante et vous donne la chance de changer de porte? Quelle est la probabilité que vous gagner en changeant la porte que vous sélectionnez à l'un des deux portes restantes parmi les trois que vous n'avez pas sélectionnées?

41. Ce problème a été posé par le chevalier de Méré et a été résolu par Blaise Pascal et Pierre de Fermat.

a) Trouvez la probabilité de rouler au moins un six quand un le dé juste est lancé quatre fois.

b) Trouver la probabilité qu'un double six apparaisse au moins une fois quand une paire de dés est lancée 24 fois. Répond à interroger le chevalier de Méré à Pascal demandant si cette probabilité est supérieure à $1/2$.

c) Est-il plus probable qu'un six apparaisse au moins une fois un dé juste est lancé quatre fois ou qu'un double six vient au moins une fois quand une paire de dés est lancée 24 fois?

Théorie des probabilités

introduction

Dans la section 7.1, nous avons introduit la notion de probabilité d'un événement.(Rappelons qu'un événement est un sous-ensemble des résultats possibles d'une expérience.) Nous avons défini la probabilité d'un événement E comme Laplace l'a fait, c'est-à-dire

$$p(E) = \frac{|E|}{|S|},$$

le nombre de résultats dans E divisé par le nombre total de résultats. Cette définition suppose que tous les résultats sont également probables. Cependant, de nombreuses expériences ont des résultats qui ne sont pas tout aussi probable. Par exemple, une pièce de monnaie peut être biaisée de sorte qu'elle remonte deux fois plus souvent que queues. De même, la probabilité que l'entrée d'une recherche linéaire soit un élément particulier d'une liste, ou n'est pas dans la liste, dépend de la façon dont l'entrée est générée. Comment modéliser la probabilité de événements dans de telles situations? Dans cette section, nous montrerons comment définir les probabilités de résultats étudier les probabilités d'expériences où les résultats peuvent ne pas être tout aussi probables.

Supposons qu'une pièce de monnaie équitable soit retournée quatre fois, et la première fois qu'elle monte en tête Donné cette information, quelle est la probabilité que les têtes reviennent trois fois? Pour répondre à cela et des questions similaires, nous introduirons le concept de *probabilité conditionnelle* . Le fait de savoir que le premier flip arrive les têtes changent la probabilité que les têtes reviennent trois fois? Si non, ces deux événements sont appelés *indépendants* , un concept étudié plus loin dans cette section.

De nombreuses questions portent sur une valeur numérique particulière associée au résultat de une expérience. Par exemple, lorsque nous retournons une pièce 100 fois, quelle est la probabilité que exactement 40 têtes apparaissent? À combien de têtes devrions-nous nous attendre? Dans cette section, nous introduira *des variables aléatoires* , qui sont des fonctions qui associent des valeurs numériques à la résultats des expériences.

Attribution de probabilités

Soit S l'espace d'échantillon d'une expérience avec un nombre fini ou dénombrable de résultats. nous attribuer une probabilité $p(s)$ à chaque résultat s . Nous exigeons que deux conditions soient remplies:

(i) $0 \leq p(s) \leq 1$ pour chaque $s \in S$

et

(ii) $$\sum_{s \in S} p(s) = 1 .$$

La condition (i) stipule que la probabilité de chaque résultat est un nombre réel non négatif non supérieur que 1. La condition (ii) stipule que la somme des probabilités de tous les résultats possibles doit être 1; c'est-à-dire que lorsque nous faisons l'expérience, il est certain que l'un de ces résultats se produit. (Notez que lorsque l'espace échantillon est infini, $\sum_{s \in S} p(s)$ est une série infinie convergente.) C'est une généralisation de la définition de Laplace dans laquelle chacun des n résultats se voit attribuer une probabilité de $1/n$. En effet, les conditions (i) et (ii) sont remplies lorsque la définition de Laplace des probabilités de des résultats tout aussi probables sont utilisés et S est fini. (Voir l'exercice 4.)

Notez que lorsqu'il y a n résultats possibles, $x_1, x_2, ..., x_n$, les deux conditions à remplir sont

(i) $0 \leq p(x_i) \leq 1$ pour $i = 1, 2, ..., n$

et

(ii) $$\sum_{i=1}^{n} p(x_i) = 1 .$$

La fonction p de l'ensemble de tous les résultats de l'espace d'échantillonnage S est appelée une **probabilité distribution** .

Pour modéliser une expérience, la probabilité $p(s)$ attribuée à un résultat s doit être égale à la limite du nombre de fois où s se produit divisé par le nombre de fois que l'expérience est effectuée, que ce nombre augmente sans limite. (Nous supposerons que toutes les expériences discutées ont des résultats prévisibles en moyenne, de sorte que cette limite existe. Nous supposons également que les résultats des essais successifs d'une expérience ne dépendent pas des résultats antérieurs.)

NOTE HISTORIQUE Le chevalier de Méré était un noble français, un joueur célèbre et un bon vivant. Il a réussi à faire des paris avec des cotes légèrement supérieures à $1/2$ (par exemple ayant au moins un six viennent en quatre lancers d'un dé juste). Sa correspondance avec Pascal l'interroge sur la probabilité d'avoir au moins un double six apparaît quand une paire de dés est lancée 24 fois, ce qui a conduit au développement de la théorie des probabilités. Selon un récit, Pascal a écrit à Fermat à propos du Chevalier disant quelque chose comme «C'est un bon gars mais, hélas, ce n'est pas un mathématicien. »

Remarque: Nous ne discuterons pas des probabilités d'événements lorsque l'ensemble des résultats n'est pas fini ou dénombrable, par exemple lorsque le résultat d'une expérience peut être n'importe quel nombre réel. Dans ces cas, le calcul intégral est généralement requis pour l'étude des probabilités d'événements.

Nous pouvons modéliser des expériences dans lesquelles les résultats sont tout aussi probables ou pas aussi probables en choisissant la fonction appropriée $p(s)$, comme l'illustre l'exemple 1.

EXEMPLE 1 Quelles probabilités devons-nous attribuer aux résultats H (têtes) et T (queues) lorsqu'une pièce est équitable est retourné? Quelles probabilités devraient être attribuées à ces résultats lorsque la pièce est biaisée afin que les têtes remontent deux fois plus souvent que les queues?

Solution: pour une pièce équitable, la probabilité que des têtes se lèvent lorsque la pièce est retournée est égale à la probabilité que la queue monte, donc les résultats sont tout aussi probables. Par conséquent, nous attribuons la probabilité de $1/2$ à chacun des deux résultats possibles, qui est, $p(H) = p(T) = 1/2$.

Pour la pièce biaisée, nous avons

$$p(H) = 2\,p(T).$$

Car

$$p(H) + p(T) = 1,$$

il s'ensuit que

$$2\,p(T) + p(T) = 3\,p(T) = 1.$$

Nous concluons que $p(T) = 1/3$, et $p(H) = 2/3$. ▲

DÉFINITION 1 Supposons que S soit un ensemble avec n éléments. La *distribution uniforme* attribue la probabilité $1/n$ à chaque élément de S.

Nous définissons maintenant la probabilité d'un événement comme la somme des probabilités des résultats dans cet événement.

DÉFINITION 2 La *probabilité* de l'événement E est la somme des probabilités des résultats dans E. C'est,

$$p(E) = \sum_{s \in E} p(s).$$

(Notez que lorsque E est un ensemble infini, $\sum_{s \in E} p(s)$ est une série infinie convergente.)

Notez que lorsqu'il y a n résultats dans l'événement E, c'est-à-dire si $E = \{a_1, a_2, ..., a_n\}$, alors $p(E) = \sum_{i=1}^{n} p(a_i)$. Notez également que la distribution uniforme attribue la même probabilité à un événement que la définition originale de Laplace de la probabilité attribue à cet événement. L'expérience de sélectionner un élément à partir d'un espace échantillon avec une distribution uniforme est appelé sélection d'un élément de S **au hasard**.

EXEMPLE 2 Supposons qu'un dé soit biaisé (ou chargé) de sorte que 3 apparaisse deux fois plus souvent que chaque autre nombre mais que les cinq autres résultats sont également probables. Quelle est la probabilité qu'un nombre impair apparaît quand on lance ce dé?

Solution: Nous voulons trouver la probabilité de l'événement $E = \{1, 3, 5\}$. Par l'exercice 2, nous avons

$$p(1) = p(2) = p(4) = p(5) = p(6) = 1/7; p(3) = 2/7.$$

Il s'ensuit que

$$p(E) = p(1) + p(3) + p(5) = 1/7 + 2/7 + 1/7 = 4/7.$$ ▲

Lorsque les résultats possibles sont tout aussi probables et qu'il existe un nombre fini de vient, la définition de la probabilité d'un événement donnée dans cette section (Définition 2) avec la définition de Laplace (Définition 1 de la section 7.1). Pour voir cela, supposons qu'il n'y ait pas n résultats tout aussi probables; chaque résultat possible a une probabilité de $1/n$, car la somme de leur les probabilités sont 1. Supposons que l'événement E contienne m résultats. Selon la définition 2,

$$p(E) = \sum_{i=1}^{m} \frac{1}{n} = \frac{m}{n}.$$

Parce que $|E| = m$ et $|S| = n$, il s'ensuit que

$$p(E) = \frac{m}{n} = \frac{|E|}{|S|}.$$

Ceci est la définition de Laplace de la probabilité de l'événement E.

Probabilités de compléments et d'unions d'événements

Les formules de probabilités de combinaisons d'événements de la section 7.1 continuent de s'appliquer lorsque nous utilisons la définition 2 pour définir la probabilité d'un événement. Par exemple, le théorème 1 de La section 7.1 affirme que

$$p(\overline{E}) = 1 - p(E),$$

où $\overline{E}$ est l'événement complémentaire de l'événement E . Cette égalité est également valable lorsque la définition 2 est utilisé. Pour voir cela, notez que parce que la somme des probabilités des n résultats possibles est 1, et chaque résultat est soit en E soit en $\overline{E}$, mais pas dans les deux, nous avons

$$\sum_{s \in S} p(s) = 1 = p(E) + p(\overline{E}).$$

Par conséquent, $p(\overline{E}) = 1 - p(E)$.

Selon la définition de Laplace, par le théorème 2 de la section 7.1, nous avons

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

chaque fois que E_1 et E_2 sont des événements dans un espace échantillon S . Cela vaut également lorsque nous définissons le capacité d'un événement comme nous le faisons dans cette section. Pour voir cela, notons que $p(E_1 \cup E_2)$ est la somme de les probabilités des résultats dans $E_1 \cup E_2$. Lorsqu'un résultat x est dans un, mais pas dans les deux, de E_1 et E_2 , $p(x)$ apparaît exactement dans l'une des sommes pour $p(E_1)$ et $p(E_2)$. Quand un le résultat x est à la fois dans E_1 et E_2 , $p(x)$ se produit dans la somme pour $p(E_1)$, dans la somme pour $p(E_2)$, et dans la somme pour $p(E_1 \cap E_2)$, donc cela se produit 1 + 1 - 1 = 1 fois sur le côté droit. Conseiller par conséquent, le côté gauche et le côté droit sont égaux.

Notez également que si les événements E_1 et E_2 sont disjoints, alors $p(E_1 \cap E_2) = 0$, ce qui implique cette

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2) = p(E_1) + p(E_2).$$

Le théorème 1 généralise cette dernière formule en fournissant une formule pour la probabilité de la union d'événements disjoints par paires.

THÉORÈME 1 Si $E_1, E_2, \ldots$ est une séquence d'événements disjoints par paire dans un espace échantillon S , alors

$$p\left(\bigcup_{je} E_i\right) = \sum_{je} p(E_i).$$

(Notez que ce théorème s'applique lorsque la séquence $E_1, E_2, \ldots$ consiste en un nombre fini ou un nombre infiniment comptable d'événements disjoints par paires.)

Nous laissons au lecteur la preuve du théorème 1 (voir exercices 36 et 37).

Probabilite conditionnelle

Supposons que nous lançons une pièce trois fois, et les huit possibilités sont également probables. En outre, supposons que nous sachions que l'événement F , que le premier flip se déclenche, se produit. Compte tenu de ces informations, quelle est la probabilité de l'événement E , qu'un nombre impair de queues apparaisse? Parce que le premier flip monte la queue, il n'y a que quatre résultats possibles: TTT , TTH , THT et THH , où H et T représentent respectivement les têtes et les queues. Un nombre impair de queues n'apparaît que pour résultats TTT et THH . Parce que les huit résultats ont une probabilité égale, chacun des quatre résultats possibles, étant donné que F se produit, devraient également avoir une probabilité égale de $1/4$. Cette suggère que nous devrions assigner la probabilité du $2/4 = 1/2$ à E , étant donné que F se produit. Cette la probabilité est appelée la **probabilité conditionnelle** de E donné F .

En général, pour trouver la probabilité conditionnelle de E étant donné F , nous utilisons F comme espace d'échantillonnage. Pour un résultat de E à se produire, ce résultat doit également appartenir à $E \cap F$. Avec cette motivation, nous faisons la définition 3.

DÉFINITION 3 Soit E et F *des* événements avec $p(F) > 0$. La *probabilité conditionnelle* de E étant F , notée par $p(E \mid F)$, est défini comme

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}.$$

EXEMPLE 3 Une chaîne de bits de longueur quatre est générée de façon aléatoire de sorte que chacune des 16 chaînes de bits de longueur quatre est tout aussi probable. Quelle est la probabilité qu'il contienne au moins deux 0 consécutifs, étant donné que son premier bit est un 0?(Nous supposons que 0 bits et 1 bits sont également probables.)

Solution: Soit E l'événement qu'une chaîne de bits de longueur quatre contient au moins deux 0 consécutifs, et soit F l'événement si le premier bit d'une chaîne de bits de longueur quatre est un 0. La probabilité qu'un chaîne de bits de longueur quatre a au moins deux 0 consécutifs, étant donné que son premier bit est un 0, est égal à

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}.$$

Parce que $E \cap F = \{0000, 0001, 0010, 0011, 0100\}$, on voit que $p(E \cap F) = 5/16$. Parce que Il y a huit chaînes de bits de longueur quatre commençant par 0, on a $p(F) = 8/16 = 1/2$. Par conséquent,

$$p(E \mid F) = \frac{5/16}{1/2} = \frac{5}{8}.$$

▲

EXEMPLE 4 Quelle est la probabilité conditionnelle qu'une famille avec deux enfants ait deux garçons, étant donné avoir au moins un garçon? Supposons que chacune des possibilités BB, BG, GB et GG soit égale probablement, où B représente un garçon et G représente une fille. (Notez que BG représente une famille avec un garçon plus âgé et une jeune fille tandis que GB représente une famille avec une fille plus âgée et un jeune garçon.)

Solution: Soit E l'événement où une famille avec deux enfants a deux garçons et F soit le cas où une famille avec deux enfants a au moins un garçon. Il s'ensuit que $E = \{BB\}$, $F = \{BB, BG, GB\}$ et $E \cap F = \{BB\}$. Parce que les quatre possibilités sont également probables, il suivant que $p(F) = 3/4$ et $p(E \cap F) = 1/4$. Nous concluons que

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)} = \frac{1/4}{3/4} = \frac{1}{3}.$$

▲

Indépendance

Supposons qu'une pièce soit retournée trois fois, comme décrit dans l'introduction de notre discussion sur probabilite conditionnelle. Le fait de savoir que le premier flip survient (événement F) modifie-t-il probabilité que la queue remonte un nombre impair de fois (événement E)? En d'autres termes, est-ce le cas que $p(E \mid F) = p(E)$? Cette égalité est valable pour les événements E et F, parce que $p(E \mid F) = 1/2$ et $p(E) = 1/2$. Parce que cette égalité est vraie, nous disons que E et F sont **des événements indépendants**. Lorsque deux événements sont indépendants, la survenance de l'un des événements ne donne aucune information sur la probabilité que l'autre événement se produise.

Parce que $p(E \mid F) = p(E \cap F)/p(F)$, demander si $p(E \mid F) = p(E)$ est identique à demandant si $p(E \cap F) = p(E)\, p(F)$. Cela conduit à la définition 4.

DÉFINITION 4 Les événements E et F sont *indépendants* si et seulement si $p(E \cap F) = p(E)\, p(F)$.

EXEMPLE 5 Supposons que E est l'événement où une chaîne de bits générée aléatoirement de longueur quatre commence par un 1 et F est l'événement où cette chaîne de bits contient un nombre pair de 1.Sont E et F indépendants, si les chaînes de 16 bits de longueur quatre sont également probables?

Solution: il y a huit chaînes de bits de longueur quatre qui commencent par une: 1000, 1001, 1010, 1011, 1100, 1101, 1110 et 1111. Il existe également huit chaînes de bits de longueur quatre qui contiennent un nombre pair: 0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111. Parce qu'il y a 16 chaînes de bits de longueur quatre, il s'ensuit que

$$p(E) = p(F) = 8/16 = 1/\text{deux}.$$

Parce que $E \cap F = \{1111, 1100, 1010, 1001\}$, nous voyons que

$$p(E \cap F) = 4/16 = 1/4.$$

Car

$$p(E \cap F) = 1/4 = (1/2)(1/2) = p(E)\, p(F),$$

nous concluons que E et F sont indépendants.

▲

La probabilité a de nombreuses applications en génétique, comme l'illustrent les exemples 6 et 7.

EXEMPLE 6 Supposons, comme dans l'exemple 4, que chacune des quatre façons dont une famille peut avoir deux enfants est également probable. Les événements E, qu'une famille avec deux enfants a deux garçons, et F, qu'une famille avec deux enfants ont au moins un garçon, indépendant?

Solution: Puisque $E = \{BB\}$, nous avons $p(E) = 1/4$. Dans l' exemple 4 nous avons montré que $p(F) = 3/4$ et en ce que $p(E \cap F) = 1/$ quatre. Mais $p(E)\,p(F) = \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16}$. Donc $p(E \cap F) = p(E)\,p(F)$, les événements E et F ne sont donc pas indépendants. ▲

EXEMPLE 7 Les événements E, qu'une famille avec trois enfants a des enfants des deux sexes, et F, sont-ils la famille a au plus un garçon, indépendant? Supposons que les huit façons dont une famille peut avoir trois les enfants sont tout aussi probables.

Solution: par hypothèse, chacune des huit façons dont une famille peut avoir trois enfants, BBB, BBG, BGB, BGG, GBB, GBG, GGB et GGG, a une probabilité de $1/8$. Parce que $E = \{BBG, BGB, BGG, GBB, GBG, GGB\}$, $F = \{BGG, GBG, GGB, GGG\}$ et $E \cap F = \{BGG, GBG, GGB\}$, il en résulte que $p(E) = 6/8 = 3/4$, $p(F) = 4/8 = 1/2$, et $p(E \cap F) = 3/8$. Parce que

$$p(E)\,p(F) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8},$$

il s'ensuit que $p(E \cap F) = p(E)\,p(F)$, donc E et F sont indépendants. (Cette conclusion peut sembler surprenant. En effet, si nous modifions le nombre d'enfants, la conclusion risque de ne plus tenir. Voir exercice 27.) ▲

INDÉPENDANCE PAIRWISE ET MUTUELLE On peut aussi définir l'indépendance des plus de deux événements. Cependant, il existe deux types d'indépendance différents, Définition 5.

DÉFINITION 5 Les événements $E_1, E_2, \ldots, E_n$ sont *indépendants par paire* si et seulement si $p(E_i \cap E_j) = p(E_i)\,p(E_j)$ pour toutes les paires d'entiers i et j avec $1 \leq i < j \leq n$. Ces événements sont *mutuellement indépendant* si $p(E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_m}) = p(E_{i_1})\,p(E_{i_2}) \cdots p(E_{i_m})$ chaque fois que i_j, $j = 1, 2, \ldots, m$, sont des entiers avec $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ et $m \geq 2$.

De la définition 5, nous voyons que chaque ensemble de n événements mutuellement indépendants est également par paires indépendant. Cependant, n événements indépendants par paire ne sont pas nécessairement mutuellement indépendants, comme nous le voyons dans l'exercice 25 des exercices supplémentaires. De nombreux théorèmes sur n événements incluent l'hypothèse que ces événements sont mutuellement indépendants, et pas seulement indépendants par paire. Nous présenterons plusieurs de ces théorèmes plus loin dans ce chapitre.

Essais de Bernoulli et distribution binomiale

Supposons qu'une expérience ne puisse avoir que deux résultats possibles. Par exemple, lorsqu'un bit est généré au hasard, les résultats possibles sont 0 et 1. Lorsqu'une pièce est retournée, le possible les résultats sont des têtes et des queues. Chaque performance d'une expérience avec deux résultats possibles est appelé un **procès Bernoulli**, après James Bernoulli, qui a fait d'importantes contributions à la probabilité théorie. En général, un résultat possible d'un procès Bernoulli est appelé un **succès** ou un **échec**. Si p est la probabilité de réussite et q est la probabilité d'échec, il s'ensuit que $p + q = 1$.

De nombreux problèmes peuvent être résolus en déterminant la probabilité de k succès lorsqu'un ex- le test consiste en n essais de Bernoulli mutuellement indépendants. (Les essais de Bernoulli sont **mutuellement indépendant** si la probabilité conditionnelle de succès d'un essai donné est de p, compte tenu des informations que ce soit sur les résultats des autres essais.) Considérons l'exemple 8.

EXEMPLE 8 Une pièce est biaisée de sorte que la probabilité de têtes est de 2/ 3. Quelle est la probabilité qu'exactement quatre les têtes se lèvent lorsque la pièce est retournée sept fois, en supposant que les flips sont indépendants?

Solution: Il y a $2^7 = 128$ résultats possibles lorsqu'une pièce est retournée sept fois. Le nombre de quatre des sept flips peuvent être des têtes est $C(7, 4)$. Parce que les sept flips sont indépendants, le probabilité de chacun de ces résultats (quatre têtes et trois queues) est $(2/3)^4 (\text{une}/3)^3$. Par conséquent, la probabilité d'apparaître exactement quatre têtes est

$$C(7, 4)(2/3)^4(\text{une}/3)^3 = \frac{35 \cdot 16}{3^7} = \frac{560}{2187}.$$

▲

En suivant le même raisonnement que celui utilisé dans l'exemple 8, nous pouvons trouver la probabilité de k succès dans n essais Bernoulli indépendants.

THÉORÈME 2 La probabilité d'exactement k succès dans n essais de Bernoulli indépendants, avec probabilité de succès p et probabilité d'échec $q = 1 - p$, est

$$C(n, k) p^k q^{n-k}.$$

Preuve: lorsque n essais de Bernoulli sont réalisés, le résultat est un n- tuple $(t_1, t_2, \ldots, t_n)$, où $t_i = S$ (pour le succès) ou $t_i = F$ (pour l'échec) pour $i = 1, 2, \ldots, n$. Parce que les n essais sont indépendant, la probabilité de chaque résultat de n essais consistant en k succès et $n - k$ échecs (dans n'importe quel ordre) est $p^k q^{n-k}$. Parce qu'il y a $C(n, k)$ n-tuples de S et F qui contiennent exactement k S, la probabilité d'exactement k succès est

$$C(n, k) p^k q^{n-k}.$$

On note $b(k; n, p)$ la probabilité de k succès dans n triples de Bernoulli indépendants als avec probabilité de succès p et probabilité d'échec $q = 1 - p$. Considéré comme un fonction de k, nous appelons cette fonction la **distribution binomiale**. Le théorème 2 nous dit que $b(k; n, p) = C(n, k) p^k q^{n-k}$.

EXEMPLE 9 Supposons que la probabilité qu'un bit 0 soit généré est 0. 9, que la probabilité qu'un bit 1 soit généré est 0 . 1, et que les bits sont générés indépendamment. Quelle est la probabilité qu'exactement huit 0 bits sont générés lorsque 10 bits sont générés?

Solution: selon le théorème 2, la probabilité de générer exactement huit bits 0 est

$$b(8; 10, 0.9) = C(10, 8)(0.9)^8(0.1)^2 = 0.1937102445.$$

▲

JAMES BERNOULLI (1654-1705) James Bernoulli (également connu sous le nom de Jacob I), est né à Bâle, en Suisse. Il est l'un des huit mathématiciens éminents de la famille Bernoulli (voir la section 10.1 pour le Bernoulli arbre généalogique des mathématiciens). Suivant le souhait de son père, James a étudié la théologie et est entré au ministère. Mais contrairement aux désirs de ses parents, il étudie également les mathématiques et l'astronomie. Il a voyagé à travers l'Europe de 1676 à 1682, s'initie aux dernières découvertes en mathématiques et sciences. De retour à Bâle en 1682, il fonde une école de mathématiques et de sciences. Il a été nommé professeur de mathématiques à l'Université de Bâle en 1687, restant dans cette position pour le reste de sa vie.

James Bernoulli est surtout connu pour l'œuvre *Ars Conjectandi*, publiée huit ans après sa mort. Dans ce travail, il a décrit les résultats connus dans la théorie des probabilités et dans l'énumération, fournissant souvent une alternative preuves de résultats connus. Ce travail comprend également l'application de la théorie des probabilités aux jeux de hasard et son introduction de la théorème connu sous le nom de **loi des grands nombres**. Cette loi stipule que si $\epsilon > 0$, lorsque n devient arbitrairement grand, la probabilité approche 1 que la fraction de fois où un événement E se produit pendant n essais est à moins de ϵ de $p(E)$.

Notez que la somme des probabilités qu'il y ait k succès lorsque n Bernoulli indépendant des essais sont effectués, pour $k = 0, 1, 2, ..., n$, est égal à

$$\sum_{k=0}^{n} C(n, k)\, p^k q^{n-k} = (p + q)^n = 1,$$

comme cela devrait être le cas. La première égalité dans cette chaîne d'égalités est une conséquence de la théorème binomial (voir section 6.4). La deuxième égalité suit parce que $q = 1 - p$.

Variables aléatoires

De nombreux problèmes concernent une valeur numérique associée au résultat d'une expérience ment. Par exemple, nous pouvons être intéressés par le nombre total d'un bit dans un généré aléatoirement chaîne de 10 bits; ou dans le nombre de fois que la queue monte quand une pièce est retournée 20 foisÀ étudier des problèmes de ce type, nous introduisons le concept d'une variable aléatoire.

DÉFINITION 6 Une *variable aléatoire* est une fonction de l'espace d'échantillonnage d'une expérience à l'ensemble de réels Nombres. C'est-à-dire qu'une variable aléatoire attribue un nombre réel à chaque résultat possible.

Remarque: Notez qu'une variable aléatoire est une fonction. Ce n'est pas une variable et ce n'est pas aléatoire! Le nom *variable aléatoire* (la traduction de *variabile casuale*) a été introduit par l'italien mathématicien FP Cantelli en 1916. À la fin des années 40, les mathématiciens W. Feller et JL Doob a lancé une pièce pour voir si les deux utiliseraient une «variable aléatoire» ou la plus appropriée terme «variable de chance». Feller a gagné; malheureusement, «variable aléatoire» a été utilisé dans les livres et depuis.

EXEMPLE 10 Supposons qu'une pièce soit lancée trois fois. Soit $X(t)$ la variable aléatoire égale à la nombre de têtes qui apparaissent lorsque t est le résultat. Alors $X(t)$ prend les valeurs suivantes:

$$X(HHH) = 3,$$
$$X(HHT) = X(HTH) = X(THH) = 2,$$
$$X(TTH) = X(THT) = X(HTT) = 1,$$
$$X(TTT) = 0.$$

▲

DÉFINITION 7 La *distribution* d'une variable aléatoire X sur un espace échantillon S est l'ensemble des paires $(r, p(X = r))$ pour tout $r \in X(S)$, où $p(X = r)$ est la probabilité que X prenne la valeur r. (L'ensemble des paires dans cette distribution est déterminée par les probabilités $p(X = r)$ pour $r \in X(S)$.)

EXEMPLE 11 Chacun des huit résultats possibles quand une pièce de monnaie juste est retourné trois fois a une probabilité de $1/8$. Ainsi, la distribution de la variable aléatoire $X(t)$ dans l'exemple 10 est déterminée par le probabilités $P(X = 3) = 1/8$, $P(X = 2) = 3/8$, $P(X = 1) = 3/8$, et $P(X = 0) = 1/8$. Conséquent, la distribution de $X(t)$ dans l' exemple 10 est l'ensemble des paires $(3, 1/8)$, $(2, 3/8)$, $(1, 3/8)$, et $(0$, une / huit$)$. ▲

EXEMPLE 12 Soit X la somme des nombres qui apparaissent quand une paire de dés est lancée. Quelles sont les valeurs de cette variable aléatoire pour les 36 résultats possibles (i, j), où i et j sont les nombres qui apparaissent sur le premier dé et le deuxième dé, respectivement, lorsque ces deux dés sont lancés?

Solution: la variable aléatoire X prend les valeurs suivantes:

$$X((1,1)) = 2,$$
$$X((1,2)) = X((2,1)) = 3,$$
$$X((1,3)) = X((2,2)) = X((3,1)) = 4,$$
$$X((1,4)) = X((2,3)) = X((3,2)) = X((4,1)) = 5,$$
$$X((1,5)) = X((2,4)) = X((3,3)) = X((4,2)) = X((5,1)) = 6,$$
$$X((1,6)) = X((2,5)) = X((3,4)) = X((4,3)) = X((5,2)) = X((6,1)) = 7,$$
$$X((2,6)) = X((3,5)) = X((4,4)) = X((5,3)) = X((6,2)) = 8,$$
$$X((3,6)) = X((4,5)) = X((5,4)) = X((6,3)) = 9,$$
$$X((4,6)) = X((5,5)) = X((6,4)) = 10,$$
$$X((5,6)) = X((6,5)) = 11,$$
$$X((6,6)) = 12.$$

▲

Nous poursuivrons notre étude des variables aléatoires dans la section 7.4, où nous montrerons comment ils peuvent être utilisés dans une variété d'applications.

Le problème de l'anniversaire

Un puzzle célèbre demande le plus petit nombre de personnes nécessaires dans une pièce pour qu'il soit plus probable qu'au moins deux d'entre eux ont le même jour de l'année que leur anniversaire. La plupart des gens trouver la réponse, que nous déterminons dans l'exemple 13, étonnamment petite. Après avoir résolu ce fameux problème, nous allons montrer comment un raisonnement similaire peut être adapté pour résoudre une question sur les fonctions de hachage.

EXEMPLE 13 **Le problème de l'anniversaire** Quel est le nombre minimum de personnes qui doivent être dans une pièce pour que la probabilité qu 'au moins deux d'entre eux ont le même anniversaire est supérieur à $1/2$?

Solution: Tout d'abord, nous énonçons certaines hypothèses. Nous supposons que les anniversaires des personnes les chambres sont indépendantes. De plus, nous supposons que chaque anniversaire est également probable et que il y a 366 jours dans l'année. (En réalité, plus de personnes naissent certains jours de l'année que d'autres, comme les jours neuf mois après certaines vacances, y compris le réveillon du Nouvel An, et ne les années ont 366 jours.)

Pour déterminer la probabilité qu'au moins deux des n personnes dans une pièce aient le même anniversaire, nous calculons d'abord la probabilité p_n que ces personnes aient toutes des anniversaires différents. Puis le la probabilité qu'au moins deux personnes aient le même anniversaire est $1-p_n$. Pour calculer p_n, on considère les anniversaires des n personnes dans un ordre fixe. Imaginez-les entrer dans la pièce un par un; nous calculerons la probabilité que chaque personne successive entrant dans la pièce ait un anniversaire différent de ceux des personnes déjà présentes.

L'anniversaire de la première personne ne correspond certainement pas à l'anniversaire de quelqu'un déjà la chambre. La probabilité que l'anniversaire de la deuxième personne soit différent de celui de la première personne est de $365/366$ parce que la deuxième personne a une date de naissance différente quand il ou elle est née un des 365 jours de l'année autre que le jour de la naissance de la première personne(L'hypothèse qu'il est également probable qu'une personne naisse l'un des 366 jours de l'année entre dans cette et les étapes suivantes.)

La probabilité que la troisième personne ait un anniversaire différent des deux anniversaires de les première et deuxième personnes ,étant donné que ces deux personnes ont des dates d' anniversaire est de $364/366$. générale, la probabilité que la j ème personne, avec $2 \leq j \leq 366$, ait un anniversaire différent de la

anniversaires des j - 1 personnes déjà dans la salle étant donné que ces j - 1 personnes ont différents les anniversaires est

$$\frac{366-(j-1)}{366} = \frac{367-j}{366}.$$

Parce que nous avons supposé que les anniversaires des personnes dans la pièce étaient indépendants, nous peut conclure que la probabilité que les n personnes dans la pièce aient des anniversaires différents est

$$p_n = \frac{365}{366}\frac{364}{366}\frac{363}{366}\cdots\frac{367-n}{366}.$$

Il s'ensuit que la probabilité que parmi n personnes il y ait au moins deux personnes avec le même anniversaire est

$$1 - p_n = 1 - \frac{365}{366}\frac{364}{366}\frac{363}{366}\cdots\frac{367-n}{366}.$$

Déterminer le nombre minimum de personnes dans la pièce afin que la probabilité qu'à moins deux d'entre eux ont le même anniversaire est supérieur à $1/2$, nous utilisons la formule que nous avons trouvé pour $1 - p_n$ pour le calculer pour des valeurs croissantes de n jusqu'à ce qu'il devienne supérieur à $1/2$. (Il y a des approches plus sophistiquées utilisant le calcul qui peuvent éliminer ce calcul, mais nous allons pas les utiliser ici.) Après un calcul considérable, nous constatons que pour $n = 22$, $1 - p_n \approx 0.475$, tandis que pour $n = 23$, $1 - p_n \approx 0.506$. Par conséquent, le nombre minimum de personnes nécessaires pour que la probabilité qu 'au moins deux personnes ont le même anniversaire est supérieure à $1/2$ est 23. ▲

La solution au problème d'anniversaire conduit à la solution de la question de l'exemple 14 sur les fonctions de hachage.

EXEMPLE 14 **Probabilité d'une collision dans les fonctions de hachage** Rappel de la section 4.5 qu'un hachage la fonction $h(k)$ est un mappage des clés (des enregistrements qui doivent être stockés dans une base de données) emplacements de stockage. Les fonctions de hachage mappent un large univers de touches (comme le 300 millions de numéros de sécurité sociale aux États-Unis) à un ensemble de stockage beaucoup plus petit Emplacements. Une bonne fonction de hachage produit peu de **collisions** , qui sont des correspondances de deux clés du même emplacement de mémoire, lorsque relativement peu d'enregistrements sont en cours de lecture dans un application. Quelle est la probabilité que deux clés ne soient pas mappées au même emplacement par un fonction de hachage, ou, en d'autres termes, qu'il n'y a pas de collisions?

Solution: pour calculer cette probabilité, nous supposons que la probabilité qu'une sélection aléatoire est mappée sur un emplacement est $1/m$, où m est le nombre d'emplacements disponibles, c'est-à-dire le la fonction de hachage distribue les clés uniformément.(En pratique, les fonctions de hachage peuvent ne pas supposition. Cependant, pour une bonne fonction de hachage, cette hypothèse devrait être proche de la correction.) De plus, nous supposons que les clés des enregistrements sélectionnés ont une probabilité égale d'être l'un des éléments de l'univers clé et que ces clés sont sélectionnées indépendamment.

Supposons que les clés soient $k_1, k_2, \ldots, k_n$. Lorsque nous ajoutons le deuxième enregistrement, la probabilité qu'il est mappé sur un emplacement différent de l'emplacement du premier enregistrement, que $h(k_2) = h(k_1)$, est $(m-1)/m$ car il y a $m-1$ emplacements libres après le premier enregistrement.le probabilité que le troisième enregistrement soit mappé sur un emplacement libre après les premier et deuxième enregistrements ont été placés sans collision est $(m-2)/m$. En général, la probabilité que le j ème enregistrement est mappé sur un emplacement libre après que les premiers $j-1$ enregistrements ont été mappés sur les emplacements $h(k_1)$, $h(k_2), \ldots, h(k_{j-1})$ sans collision est $(m-(j-1))/m$ car $j-1$ des m emplacements sont pris.

Étant donné que les clés sont indépendantes, la probabilité que toutes les n clés soient mappées à différents emplacements est

$$p_n = \frac{m-1}{m} \cdot \frac{m-2}{m} \cdot \ldots \cdot \frac{m-n+1}{m}.$$

Il s'ensuit que la probabilité qu'il y ait au moins une collision, c'est-à-dire qu'au moins deux clés sont mappé au même emplacement, est

$$1 - p_n = 1 - \frac{m-1}{m} \cdot \frac{m-2}{m} \cdot \ldots \cdot \frac{m-n+1}{m}.$$

Les techniques de calcul peuvent être utilisées pour trouver la plus petite valeur de n étant donné une valeur de m telle que la probabilité d'une collision est supérieure à un seuil particulier. On peut montrer que le le plus petit entier n tel que la probabilité de collision est supérieure à $1/2$ est d' environ $n = 1.177\sqrt{m}$. Par exemple, lorsque $m = 1{,}000{,}000$, le plus petit entier n tel que la probabilité de collision est supérieure à $1/2$ est 1178. ▲

Algorithmes de Monte Carlo

Les algorithmes discutés jusqu'à présent dans ce livre sont tous déterministes. Autrement dit, chaque algorithme toujours procède de la même manière chaque fois que la même entrée est donnée.Cependant, il existe de nombreuses situations où nous aimerions qu'un algorithme fasse un choix aléatoire en une ou plusieurs étapes.Tel que la situation se présente lorsqu'un algorithme déterministe devrait passer par un nombre énorme, ou même un nombre inconnu, de cas possibles. Algorithmes qui font des choix aléatoires sur un ou plusieurs les étapes sont appelées **algorithmes probabilistes** . Nous allons discuter d'une classe particulière de probabiliste algorithmes de cette section, à savoir les **algorithmes de Monte Carlo** , pour les problèmes de décision. Monte Les algorithmes de Carlo produisent toujours des réponses aux problèmes, mais une faible probabilité demeure que ces réponses peuvent être incorrectes. Cependant, la probabilité que la réponse soit incorrecte diminue rapidement lorsque l'algorithme effectue un calcul suffisant. Les problèmes de décision ont soit «Vrai» ou «faux» comme réponse. La dénomination «Monte Carlo» fait référence au célèbre

Méthodes de Monte Carlo

ont été inventés pour aider développer le premier nucléaire armes.

casino à Monaco; l'utilisation de l'aléatoire et les processus répétitifs dans ces algorithmes font les similaires à certains jeux de hasard.Ce nom a été introduit par les inventeurs de Monte Méthodes de Carlo, notamment Stan Ulam, Enrico Fermi et John von Neumann.

Un algorithme de Monte Carlo pour un problème de décision utilise une séquence de tests.La probabilite que l'algorithme répond correctement au problème de décision à mesure que de nouveaux tests sont effectués en dehors. À chaque étape de l'algorithme, les réponses possibles sont «vraies», ce qui signifie que la réponse est "vrai" et aucune itération supplémentaire n'est nécessaire, ou "inconnue", ce qui signifie que la réponse pourrait être «vrai» ou «faux». Après avoir exécuté toutes les itérations dans un tel algorithme, la finale la réponse produite est «vraie» si au moins une itération donne la réponse «vraie», et la réponse est «Faux» si chaque itération donne la réponse «inconnu». Si la bonne réponse est «fausse», alors le l'algorithme répond «faux», car chaque itération donnera «inconnu». Cependant, si la bonne réponse est «vrai», alors l'algorithme pourrait répondre «vrai» ou «faux», car il peut être possible que chaque itération produise la réponse «inconnue» même si la réponse correcte était «vrai». Nous montrerons que cette possibilité devient extrêmement improbable car le nombre de tests augmente.

Supposons que p soit la probabilité que la réponse d'un test soit «vraie», étant donné que la réponse est "vrai". Il s'ensuit que $1-p$ est la probabilité que la réponse soit "inconnue", étant donné que la réponse est «vraie». Parce que l'algorithme répond «faux» lorsque toutes les n itérations donnent la réponse «Inconnu» et les itérations effectuent des tests indépendants, la probabilité d'erreur est $(1-p)^n$. Lorsque $p = 0$, cette probabilité se rapproche de 0 lorsque le nombre de tests augmente.Par conséquent, le probabilité que l'algorithme réponde «vrai» lorsque la réponse est «vraie» approche 1.

EXEMPLE 15 **Contrôle qualité** (Cet exemple est adapté de [AhUl95].) Supposons qu'un fabricant ordonne les puces de processeur par lots de taille n , où n est un entier positif. Le fabricant de puces n'a testé que certains de ces lots pour s'assurer que toutes les puces du lot sont bonnes (remplacement des puces défectueuses trouvées lors des tests par de bonnes).Dans des lots non testés auparavant, la probabilité qu'une puce particulière soit mauvaise est de 0. 1 lors de tests aléatoires est fait. Le fabricant de PC veut décider si toutes les puces d'un lot sont bonnes.À

Pour ce faire, le fabricant de PC peut tester chaque puce dans un lot pour voir si elle est bonne.cependant, cela nécessite n tests. En supposant que chaque test puisse être effectué en temps constant, ces tests nécessitent $O(n)$ secondes. Le fabricant du PC peut-il déterminer si un lot de puces a été testé par le fabricant de puces en utilisant moins de temps?

Solution: nous pouvons utiliser un algorithme de Monte Carlo pour déterminer si un lot de puces a été testé par le fabricant de puces tant que nous sommes prêts à accepter une certaine probabilité d'erreur.le algorithme est configuré pour répondre à la question: «Ce lot de puces n'a-t-il pas été testé par le fabricant de puces? »Il procède en sélectionnant successivement des puces au hasard dans le lot et en testant les un par un. Lorsqu'une puce défectueuse est rencontrée, l'algorithme répond «vrai» et s'arrête.Si une puce testée est bonne, l'algorithme répond «inconnu» et passe à la puce suivante. Après l'algorithme a testé un nombre spécifié de puces, disons k puces, sans obtenir de réponse de «Vrai», l'algorithme se termine par la réponse «faux»; c'est-à-dire que l'algorithme conclut que le lot est bon, c'est-à-dire que le fabricant de puces a testé toutes les puces du lot.

La seule façon pour cet algorithme de répondre incorrectement est de conclure qu'un test non testé lot de puces a été testé par le fabricant de puces. La probabilité qu'une puce soit bonne, mais que il provient d'un lot non testé, est $1 - 0.1 = 0.9$. Parce que les événements de test de différentes puces à partir d'un lot sont indépendants, la probabilité que toutes les k étapes de l'algorithme produisent la réponse «Inconnu», étant donné que le lot de puces n'est pas testé, est égal à 0.9^k.

En prenant k assez grand, nous pouvons rendre cette probabilité aussi petite que nous le voulons.Par exemple, en testant 66 puces, la probabilité que l'algorithme décide qu'un lot a été testé par le le fabricant de puces est 0.9^{66} , ce qui est inférieur à 0.001. Autrement dit, la probabilité est inférieure à 1 sur 1000 que l'algorithme n'a pas répondu correctement. Notez que cette probabilité est indépendante de n , la nombre de puces dans un lot. Autrement dit, l'algorithme de Monte Carlo utilise un nombre constant, ou $O(1)$, teste et nécessite $O(1)$ secondes, quel que soit le nombre de puces dans un lot. Tant que le PC fabricant peut vivre avec un taux d'erreur inférieur à 1 sur 1000, l'algorithme de Monte Carlo sauver le fabricant de PC de nombreux tests.Si un taux d'erreur plus faible est nécessaire, le fabricant du PC peut tester plus de puces dans chaque lot; le lecteur peut vérifier que 132 tests abaissent le taux d'erreur à moins de 1 à 1 , 000 , 000. ▲

EXEMPLE 16 **Test probabiliste de primauté** Au chapitre 4, nous avons remarqué qu'un entier composite, c'est-à-dire un entier supérieur à un qui n'est pas premier, passe le test de Miller (voir le préambule de l'exercice 44 dans la section 4.4) pour moins de $n/4$ bases b avec $1 < b < n$. Cette observation est à la base de un algorithme de Monte Carlo pour déterminer si un entier supérieur à un est premier.Car les nombres premiers importants jouent un rôle essentiel dans la cryptographie à clé publique (voir la section 4.6), générer de grands nombres premiers rapidement est devenu extrêmement important.

Le but de l'algorithme est de décider de la question «Est-ce que n est composite?» Étant donné un entier n supérieur à un, nous sélectionnons un entier b au hasard avec $1 < b < n$ et déterminons si n passe le test de Miller à la base b . Si n échoue au test, la réponse est «vraie» car n doit être composite, et l'algorithme se termine. Sinon, nous effectuons le test k fois, où k est positif entier. Chaque fois que nous sélectionnons un entier aléatoire b et déterminons si n passe le test de Miller à la base b . Si la réponse est «inconnue» à chaque étape, l'algorithme répond «faux», c'est-à-dire qu'il dit que n n'est pas composite, de sorte qu'il est premier. La seule possibilité pour l'algorithme de retourner un une réponse incorrecte se produit lorsque n est composite, et la réponse «inconnu» est la sortie à chaque des k itérations. La probabilité qu'un entier composite n réussisse le test de Miller pour un la base b sélectionnée est inférieure à $1/4$. Parce que l'entier b avec $1 < b < n$ est sélectionné au hasard à chaque itération et ces itérations sont indépendantes, la probabilité que n soit composite mais la répond algorithme que n est premier est inférieure à $(une/quatre)^k$. En prenant k pour être suffisamment grand, nous peut rendre cette probabilité extrêmement faible. Par exemple, avec 10 itérations, la probabilité que l'algorithme décide que n est premier quand il est vraiment composite est inférieure à 1 à 1, 000 , 000. Avec 30 itérations, cette probabilité tombe à moins de 1 sur 10^{18} , un événement extrêmement improbable.

Un nombre qui passe plusieurs itérations d'un primalité probabiliste test est appelé un *industriel force première*, même bien qu'il puisse être composite.

Pour générer de grands nombres premiers, disons avec 200 chiffres, nous choisissons au hasard un entier n avec 200 chiffres et exécutez cet algorithme, avec 30 itérations. Si l'algorithme décide que n est premier, nous

peut l'utiliser comme l'un des deux nombres premiers utilisés dans une clé de chiffrement pour le cryptosystème RSA. Si n est en fait composite et est utilisé dans le cadre de la clé, les procédures utilisées pour déchiffrer les messages seront ne produit pas le message crypté d'origine. La clé est ensuite jetée et deux nouveaux possibles des nombres premiers sont utilisés. ▲

La méthode probabiliste

Nous avons discuté des preuves d'existence dans le chapitre 1 et illustré la différence entre constructif preuves d'existence et preuves d'existence non constructives. La méthode probabiliste, introduite par Paul Erd˝os et Alfréd Rényi, est une technique puissante qui peut être utilisée pour créer des preuves d'existence. Pour utiliser la méthode probabiliste pour prouver les résultats sur un ensemble S , comme le existence d'un élément dans S avec une propriété spécifiée, nous attribuons des probabilités aux éléments de S . Nous utilisons ensuite les méthodes de la théorie des probabilités pour prouver les résultats sur les éléments de S . En particulier, nous pouvons montrer qu'un élément avec une propriété spécifiée existe en montrant que le la probabilité qu'un élément $x \in S$ ait cette propriété est positive. La méthode probabiliste est basée sur la déclaration équivalente dans le théorème 3.

THÉORÈME 3 **LA MÉTHODE PROBABILISTE** Si la probabilité qu'un élément choisi au hasard d'un S n'a pas de propriété particulière est inférieure à 1, il existe un élément dans S avec cette propriété.

Une preuve d'existence basée sur la méthode probabiliste n'est pas constructive car elle ne trouve pas un élément particulier avec la propriété souhaitée.

Nous illustrons la puissance de la méthode probabiliste en trouvant une borne inférieure pour le Ramsey nombre $R(k, k)$. Rappelons à la section 6.2 que $R(k, k)$ est égal au nombre minimum de personnes à une partie doit s'assurer qu'il y a au moins k amis ou k ennemis mutuels (en supposant que deux personnes sont des amis ou des ennemis).

THÉORÈME 4 Si k est un entier avec $k \geq 2$, alors $R(k, k) \geq 2^{k/2}$.

Preuve: On note que le théorème est valable pour $k = 2$ et $k = 3$ car $R(2, 2) = 2$ et $R(3, 3) = 6$, comme indiqué à la section 6.2. Supposons maintenant que $k \geq 4$. Nous allons utiliser la méthode probabiliste pour montrer que s'il y a moins de $2^{k/2}$ personnes lors d'une fête, il est possible qu'aucun k ne soit mutuel amis ou ennemis mutuels. Cela montrera que $R(k, k)$ est au moins $2^{k/2}$.

Pour utiliser la méthode probabiliste, nous supposons qu'il est également probable que deux personnes amis ou ennemis. (Notez que cette hypothèse n'a pas besoin d'être réaliste.) Supposons qu'il sont n personnes à la fête. Il s'ensuit qu'il existe $\binom{n}{k}$ différents ensembles de k personnes à ce partie, que nous listons comme $S_1, S_2, \ldots, S_{\binom{n}{k}}$. Soit E_i l'événement où toutes les k personnes de S_i sont eileurs amis ou ennemis communs. La probabilité qu'il y ait soit k amis mutuels ou k ennemis mutuels parmi les n personnes est égal à $p(\bigcup_{i=1}^{\binom{n}{k}} E_i)$.

Selon notre hypothèse, il est également probable que deux personnes soient des amis ou des ennemis. La probabilité que deux personnes soient amis est égale à la probabilité qu'elles soient ennemies; tous les deux probabilités égales à $1/2$. De plus, il existe $\binom{k}{2} = k(k-1)/2$ paires de personnes dans S_i car il y a k personnes à S_i . Par conséquent, la probabilité que toutes les k personnes dans S_i soient des amis mutuels et probabilité que tous les k personnes , S_i sont tous deux égaux ennemis mutuels $(une/2)^{k(k-1)/2}$. Il s'ensuit que $p(E_i) = 2(1/2)^{k(k-1)/2}$.

La probabilité qu'il y ait k amis mutuels ou k ennemis mutuels dans le groupe de n les gens est égal à $p\left(\bigcup_{i=1}^{\binom{n}{k}} E_i\right)$. En utilisant l'inégalité de Boole (exercice 15), il s'ensuit que

$$p\left(\bigcup_{i=1}^{\binom{n}{k}} E_i\right) \leq \sum_{i=1}^{\binom{n}{k}} p(E_i) = \binom{n}{k} \cdot 2\left(\frac{1}{2}\right)^{k(k-1)/2}.$$

Par l'exercice 17 de la section 6.4, nous avons $\binom{n}{k} \leq n^k / 2^{k-1}$. Par conséquent,

$$\binom{n}{k} 2\left(\frac{1}{2}\right)^{k(k-1)/2} \leq \frac{n^k}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2}.$$

Maintenant, si $n < 2^{k/2}$ nous avons

$$\frac{n^k}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2} < \frac{2^{k(k/2)}}{2^{k-1}} 2\left(\frac{1}{2}\right)^{k(k-1)/2} = 2^{2-(k/2)} \leq 1,$$

où la dernière étape suit car $k \geq 4$.

Nous pouvons maintenant conclure que $p\left(\bigcup_{i=1}^{\binom{n}{k}} E_i\right) < 1$ lorsque $k \geq 4$. Par conséquent, la probabilité de la événement complémentaire, qu'il n'y a aucun ensemble de k amis ou ennemis mutuels au est supérieur à 0. Il s'ensuit que si $n < 2^{k/2}$, il y a au moins un ensemble tel qu'aucun sous-ensemble des k personnes sont des amis ou des ennemis mutuels.

Des exercices

1. Quelle probabilité attribuer au résultat de têtes quand une pièce biaisée est lancée, si les têtes sont trois fois aussi susceptibles de venir que les queues? Quelle probabilité devrait être attribué à l'issue des queues?

2. Trouvez la probabilité de chaque résultat lorsqu'un dé chargé est lancé, si un 3 est deux fois plus susceptible d'apparaître que chacun des cinq autres numéros sur le dé.

3. Trouvez la probabilité de chaque résultat lorsqu'un dé biaisé est roulé, si rouler un 2 ou rouler un 4 est trois fois plus probable comme rouler chacun des quatre autres nombres sur le dé et il est également susceptible de lancer un 2 ou un 4.

4. Montrez que les conditions (i) et (ii) sont remplies dans le cadre du définition de la probabilité, lorsque les résultats sont également probable.

5. Une paire de dés est chargée. La probabilité qu'un 4 apparaisse sur la première matrice est de $2/7$, et la probabilité qu'un 3 apparaît sur le deuxième dé est $2/7$. Autres résultats pour chaque dé apparaître avec la probabilité $1/7$. Quelle est la probabilité de 7 apparaissant comme la somme des nombres lorsque les deux dés sont roulés?

6. Quelle est la probabilité de ces événements lorsque nous sélectionner une permutation de $\{1, 2, 3\}$?

a) 1 précède 3.
b) 3 précède 1.
c) 3 précède 1 et 3 précède 2.

7. Quelle est la probabilité de ces événements lorsque nous sélectionner une permutation de $\{1, 2, 3, 4\}$?

a) 1 précède 4.
b) 4 précède 1.
c) 4 précède 1 et 4 précède 2.
d) 4 précède 1, 4 précède 2 et 4 précède 3.
e) 4 précède 3 et 2 précède 1.

8. Quelle est la probabilité de ces événements lorsque nous sélectionner une permutation de $\{1, 2, ..., n\}$ où $n \geq 4$?

a) 1 précède 2.
b) 2 précède 1.
c) 1 précède immédiatement 2.
d) n précède 1 et $n-1$ précède 2.
e) n précède 1 et n précède 2.

9. Quelle est la probabilité de ces événements lorsque nous sélectionner une permutation des 26 lettres minuscules de l'Enalphabet glish?

a) La permutation se compose des lettres en sens inverse ordre phabétique.
b) z est la première lettre de la permutation.
c) z précède a dans la permutation.
d) a précède immédiatement z dans la permutation.
e) a précède immédiatement m, qui précède immédiatement cède z dans la permutation.
f) m, n et o sont à leur place d'origine dans le permutation.

10. Quelle est la probabilité de ces événements lorsque nous sélectionner une permutation des 26 lettres minuscules de l'En-alphabet glish?

a) Les 13 premières lettres de la permutation sont en alphabet-ordre ical.
b) *a* est la première lettre de la permutation et *z* est la dernière lettre.
c) *a* et *z* sont côte à côte dans la permutation.
d) *a* et *b* ne sont pas côte à côte dans la permutation.
e) *a* et *z* sont séparés par au moins 23 lettres dans la mutation.
f) *z* précède *a* et *b* dans la permutation.

11. Supposons que *E* et *F* sont des événements tels que $p(E) = 0.7$ et $p(F) = 0.5$. Montrez que $p(E \cup F) \geq 0.7$ et $p(E \cap F) \geq 0.2$.

12. Supposons que *E* et *F* sont des événements tels que $p(E) = 0.8$ et $p(F) = 0.6$. Montrez que $p(E \cup F) \geq 0.8$ et $p(E \cap F) \geq 0.4$.

13. Montrer que si *E* et *F* sont des événements, alors $p(E \cap F) \geq p(E) + p(F) - 1$. Ceci est connu sous le **nom de Bonferroni l'égalité** .

14. Utilisez l'induction mathématique pour prouver le eralisation de l'inégalité de Bonferroni:

$$p(E_1 \cap E_2 \cap \cdots \cap E_n)$$
$$\geq p(E_1) + p(E_2) + \cdots + p(E_n) - (n - 1),$$

où $E_1, E_2, \ldots, E_n$ sont *n* événements.

15. Montrer que si $E_1, E_2, \ldots, E_n$ sont des événements d'un échantillon fini plein d'espace,

$$p(E_1 \cup E_2 \cup \cdots \cup E_n)$$
$$\leq p(E_1) + p(E_2) + \cdots + p(E_n).$$

C'est ce qu'on appelle **l'inégalité de Boole** .

16. Montrez que si *E* et *F* sont des événements indépendants, alors $\bar{E}$ et $\bar{F}$ sont également des événements indépendants.

17. Si *E* et *F* sont des événements indépendants, prouver ou infirmer que $\bar{E}$ et *F* sont nécessairement des événements indépendants.

Dans les exercices 18, 20 et 21, supposons que l'année compte 366 jours et tous les anniversaires sont également probables. Dans l'exercice 19, supposez-le est également probable qu'une personne naisse au cours d'un mois donné l'année.

18. a) Quelle est la probabilité que deux personnes choisies au dom sont nés le même jour de la semaine?
b) Quelle est la probabilité que dans un groupe de *n* personnes choisis au hasard, il y en a au moins deux nés sur le même jour de la semaine?
c) Combien de personnes choisies au hasard sont nécessaires pour faire la plus grande probabilité de $1/2$, que il y a au au moins deux personnes nées le même jour de la semaine?

19. a) Quelle est la probabilité que deux personnes choisies au dom sont nés au cours du même mois de l'année?
b) Quelle est la probabilité que dans un groupe de *n* personnes choisis au hasard, il y en a au moins deux nés dans le même mois de l'année?
c) Combien de personnes choisies au hasard sont nécessaires pour faire la plus grande probabilité de $1/2$, que il y a au au moins deux personnes nées le même mois de l'année?

20. Trouvez le plus petit nombre de personnes que vous devez choisir au hasard de sorte que la probabilité qu'au moins l'un d'entre eux a fête son anniversaire aujourd'hui est supérieure à $1/2$.

21. Trouvez le plus petit nombre de personnes que vous devez choisir au hasard de sorte que la probabilité qu'au moins deux d'entre eux sont tous deux nés le 1er Avril est supérieur à $1/2$.

∗ **22.** Le 29 février ne se produit que pendant les années bissextiles. Années divisibles par 4, mais pas par 100, sont toujours des années bissextiles. Années divisées par 100, mais pas par 400, ne sont pas des années bissextiles, mais des années divisible par 400 sont des années bissextiles.

a) Quelle distribution de probabilité pour les anniversaires devrait être utilisé pour refléter la fréquence du 29 février?
b) En utilisant la distribution de probabilité de la partie (a), est la probabilité que dans un groupe de *n* personnes au moins deux ont le même anniversaire?

23. Quelle est la probabilité conditionnelle qu'exactement quatre têtes apparaître lorsqu'une pièce de monnaie équitable est lancée cinq fois, étant donné que le premier flip est venu des têtes?

24. Quelle est la probabilité conditionnelle qu'exactement quatre têtes apparaître lorsqu'une pièce de monnaie équitable est lancée cinq fois, étant donné que le premier flip est venu pile?

25. Quelle est la probabilité conditionnelle qu'une génération aléatoire La chaîne de bits de longueur quatre contient au moins deux con-0 secutif, étant donné que le premier bit est un 1? (Supposons que les probabilités de 0 et de 1 sont les mêmes.)

26. Soit *E* l'événement qu'une chaîne de bits générée aléatoirement de longueur trois contient un nombre impair de 1, et soit *F* être l'événement où la chaîne commence par 1. Sont *E* et *F* indépendant?

27. Soit *E* et *F* les événements qu'une famille de *n* enfants a enfants des deux sexes et a au plus un garçon, respectivement activement. Sont *E* et *F* indépendant si

a) $n = 2$? **b)** $n = 4$? **c)** $n = 5$?

28. Supposons que la probabilité qu'un enfant soit un garçon est de 0,51 et que les sexes des enfants nés dans une famille sont indépendant. Quelle est la probabilité qu'une famille de cinq personnes les enfants a

a) exactement trois garçons?
b) au moins un garçon?
c) au moins une fille?
d) tous les enfants du même sexe?

29. Un groupe de six personnes joue le jeu de «l'étranger» pour déterminer qui achètera des rafraîchissements. Chaque personne retourne une juste monnaie. S'il y a une personne dont l'issue n'est pas comme tout autre membre du groupe, cette per-le fils doit acheter les rafraîchissements. Quelle est la probabilité qu'il y a une personne étrange après que les pièces ont été retournées une fois que?

30. Trouver la probabilité qu'une chaîne de bits générée aléatoirement de longueur 10 ne contient pas de 0 si les bits sont indépendants et si

a) un bit 0 et un bit 1 sont également probables.
b) la probabilité qu'un bit soit un 1 est de 0,6.
c) la probabilité que le *i* ième bit est un 1 est une / deux ^{je} pour $i = 1, 2, 3, \ldots, 10$.

31. Trouvez la probabilité qu'une famille avec cinq enfants pas de garçon, si le sexe des enfants est indépendant et si

a) un garçon et une fille sont également susceptibles.

b) la probabilité d'un garçon est de 0,51.

c) la probabilité que le i ème enfant soit un garçon est $0.51 - (i/100)$.

32. Trouver la probabilité qu'une chaîne de bits générée aléatoirement de longueur 10 commence par un 1 ou se termine par un 00 pour le même conditions que dans les parties (a), (b) et (c) de l'exercice 30, si les bits sont générés indépendamment.

33. Trouver la probabilité que le premier enfant d'une famille avec cinq enfants est un garçon ou que les deux derniers enfants du la famille sont des filles, pour les mêmes conditions que dans les parties a), (b) et (c) de l'exercice 31.

34. Trouver chacune des probabilités suivantes lorsque vous n indépen- essais Bernoulli sont effectués avec une probabilité de succès p .

a) la probabilité d'absence de succès

b) la probabilité d'au moins un succès

c) la probabilité d'au plus un succès

d) la probabilité d'au moins deux succès

35. Trouver chacune des probabilités suivantes lorsque vous n indépen- essais Bernoulli sont effectués avec une probabilité de succès p .

a) la probabilité d'absence de défaillances

b) la probabilité d'au moins une défaillance

c) la probabilité d'au plus un échec

d) la probabilité d'au moins deux échecs

36. Utiliser l'induction mathématique pour prouver que si $E_1, E_2, \ldots, E_n$ est une séquence de n paires disjointes événements dans un espace échantillon S , où n est un entier positif, alors $p(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} p(E_i)$.

∗ **37.** (*Nécessite un calcul*) Montrez que si $E_1, E_2, \ldots$ est un infini séquence d'événements disjoints par paire dans un espace échantillon S , alors $p(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} p(E_i)$. [*Astuce:* utilisez l'exercice 36 et prendre des limites.]

38. Une paire de dés est lancée dans un endroit éloigné et lorsque vous demander à un observateur honnête si au moins un dé est apparu six, cet observateur honnête répond par l'affirmative.

a) Quelle est la probabilité que la somme des nombres qui est venu sur les deux dés est sept, étant donné les informations informations fournies par l'observateur honnête?

b) Supposons que l'observateur honnête nous dise qu'au moins un dé est venu cinq. Quelle est la probabilité que la somme du nombre qui est venu sur les dés est sept, étant donné cette information?

∗∗ **39.** Cet exercice utilise la méthode probabiliste pour prouver résultat sur les tournois à tour de rôle. Dans un **tournoi à la ronde tournoi** avec m joueurs, tous les deux joueurs jouent un jeu dans lequel un joueur gagne et l'autre perd.

Nous voulons trouver des conditions sur des entiers positifs m et k avec $k < m$ tel qu'il est possible pour les résultats du tournoi d'avoir la propriété que pour chaque set de k joueurs, il y a un joueur qui bat chaque membre dans cet ensemble. Afin que nous puissions utiliser un raisonnement probabiliste pour tirer des conclusions sur les tournois à tour de rôle, nous supposons que lorsque deux joueurs s'affrontent, il est tout aussi probable que l'un ou l'autre joueur gagne la partie et nous supposons que le les résultats des différents jeux sont indépendants. Que E soit l'événement que pour chaque set S avec k joueurs, où k est un entier positif inférieur à m , il y a un joueur qui a battu tous les k joueurs en S .

a) Montrer que $p(E) \leq \sum_{j=1}^{\binom{m}{k}} p(F_j)$, où F_j est l'événement qu'il n'y a pas de joueur qui bat tous les k joueurs de la j e mis dans une liste des $\binom{m}{k}$ ensembles de k joueurs.

b) Montrer que la probabilité de F_j est $(1-2^{-k})^{m-k}$.

c) Conclure des parties (a) et (b) que $p(E) \leq \binom{m}{k}(1-2^{-k})^{m-k}$ et, par conséquent, qu'il doit être un tournoi avec la propriété décrite si $\binom{m}{k}(1-2^{-k})^{m-k} < 1$.

d) Utilisez la partie (c) pour trouver des valeurs de m telles qu'il tournoi avec m joueurs tel que pour chaque set S de deux joueurs, il y a un joueur qui a battu les deux joueurs en S . Répétez l'opération pour des ensembles de trois joueurs.

∗ **40.** Concevoir un algorithme de Monte Carlo qui détermine si une permutation des nombres entiers 1 à n a déjà été trié (c'est-à-dire qu'il est en ordre croissant), ou à la place, est un permutation dom. Une étape de l'algorithme devrait répondre «Vrai» s'il détermine que la liste n'est pas triée et «inconnue» autrement. Après k étapes, l'algorithme décide que l'in- les tegers sont triés si la réponse est «inconnue» à chaque étape. Montrez qu'au fur et à mesure que le nombre de pas augmente, le bilité que l'algorithme produit une réponse incorrecte est extrêmement petit. [*Astuce:* pour chaque étape, vérifiez si certains éléments sont dans le bon ordre. Assurez-vous que les tests sont indépendants.]

41. Utilisez le pseudocode pour écrire la primauté probabiliste test décrit dans l'exemple 16.

Théorème de Bayes

introduction

Il y a plusieurs fois où nous voulons évaluer la probabilité qu'un événement particulier se produise sur base de preuves partielles. Par exemple, supposons que nous connaissions le pourcentage de personnes qui ont une maladie particulière pour laquelle il existe un test de diagnostic très précis.Les personnes dont le test est positif cette maladie aimerait connaître la probabilité qu'ils en soient réellement atteints. Dans cette section nous introduisons un résultat qui peut être utilisé pour déterminer cette probabilité, à savoir la probabilité que une personne a la maladie étant donné que cette personne est positive. Pour utiliser ce résultat, nous allons besoin de connaître le pourcentage de personnes qui ne sont pas atteintes de la maladie mais dont le test est positif et le pourcentage de personnes atteintes de la maladie mais dont le test est négatif.

De même, supposons que nous connaissions le pourcentage de messages électroniques entrants qui sont du spam.nous verra que nous pouvons déterminer la probabilité qu'un e-mail entrant soit du spam en utilisant l'occurrence de mots dans le message. Pour déterminer cette probabilité, nous devons connaître pourcentage de messages entrants qui sont du spam, pourcentage de messages indésirables dans lesquels chacun de ces mots apparaît, et le pourcentage de messages qui ne sont pas du spam dans lequel chacun ces mots se produisent.

Le résultat que nous pouvons utiliser pour répondre à de telles questions s'appelle le théorème de Bayes et remonte au XVIIIe siècle. Au cours des deux dernières décennies, le théorème de Bayes a été largement utilisé pour estimer les probabilités sur la base de preuves partielles dans des domaines aussi divers que médecine, droit, apprentissage automatique, ingénierie et développement de logiciels.

Théorème de Bayes

Nous illustrons l'idée derrière le théorème de Bayes avec un exemple qui montre que lorsque supplémentaire l'information est disponible, nous pouvons obtenir une estimation plus réaliste qu'un événement particulier se produit. Autrement dit, supposons que nous connaissons $p(F)$, la probabilité qu'un événement F se produise, mais nous avons des connaissances qu'un événement E se produit. Ensuite, la probabilité conditionnelle que F se produit étant donné que E se produit, $p(F \mid E)$, est une estimation plus réaliste que $p(F)$ que F se produit. Dans l'exemple 1, nous verrons que nous pouvons trouver $p(F \mid E)$ lorsque nous connaissons $p(F)$, $p(E \mid F)$ et $p(E \mid \overline{F})$.

EXEMPLE 1 Nous avons deux cases. Le premier contient deux boules vertes et sept boules rouges; le second contient quatre boules vertes et trois boules rouges. Bob sélectionne une balle en choisissant d'abord l'une des deux cases Aléatoire. Il sélectionne ensuite au hasard l'une des boules de cette case. Si Bob a sélectionné une balle rouge, quelle est la probabilité qu'il ait sélectionné une balle dans la première case?

Solution: Soit E l'événement que Bob a choisi une balle rouge; $\overline{E}$ est l'événement que Bob a choisi une boule verte. Soit F l'événement que Bob a choisi une balle dans la première case; $\overline{F}$ est l'événement qui Bob a choisi une balle dans la deuxième case. Nous voulons trouver $p(F \mid E)$, la probabilité que le la balle que Bob a choisie est venue de la première boîte, étant donné qu'elle est rouge Par la définition du conditionnel probabilité, on a $p(F \mid E) = p(F \cap E) / p(E)$. Pouvons-nous utiliser les informations fournies pour déterminer à la fois $p(F \cap E)$ et $p(E)$ afin que nous puissions trouver $p(F \mid E)$?

Tout d'abord, notez que parce que la première boîte contient sept boules rouges sur un total de neuf boules, on sait que $p(E \mid F) = 7/9$. De même, parce que la deuxième case contient trois boules rouges sur un total de sept boules, nous savons que $p(E \mid \overline{F}) = 3/7$. Nous avons supposé que Bob sélectionne un boîte au hasard, donc $p(F) = p(\overline{F}) = 1/2$. Parce que $p(E \mid F) = p(E \cap F) / p(F)$, il s'ensuit que $p(E \cap F) = p(E \mid F)\, p(F) = \frac{7}{9} \cdot \frac{1}{2} = \frac{7}{18}$ [comme nous l'avons remarqué plus tôt, c'est l'une des quantités nous devons trouver pour déterminer $p(F \mid E)$]. De même, comme $p(E \mid \overline{F}) = p(E \cap \overline{F}) / p(\overline{F})$, il s'ensuit que $p(E \cap \overline{F}) = p(E \mid \overline{F})\, p(\overline{F}) = \frac{3}{7} \cdot \frac{1}{2} = \frac{3}{14}$.

Nous pouvons maintenant trouver $p(E)$. Notez que $E = (E \cap F) \cup (E \cap \overline{F})$, où $E \cap F$ et $E \cap \overline{F}$ sont ensembles disjoints. (Si x appartient à la fois à $E \cap F$ et à $E \cap \overline{F}$, alors x appartient à la fois à F et $\overline{F}$, qui est impossible.) Il s'ensuit que

$$p(E) = p(E \cap F) + p(E \cap \overline{F}) = \frac{\text{sept}}{18} + \frac{3}{14} = \frac{49}{126} + \frac{27}{126} = \frac{76}{126} = \frac{38}{63}.$$

Nous avons maintenant trouvé à la fois $p(F \cap E) = 7/18$ et $p(E) = 38/63$. Nous concluons que

$$p(F \mid E) = \frac{p(F \cap E)}{p(E)} = \frac{7/18}{38/63} = \frac{49}{76} \approx 0.645.$$

Avant d'avoir des informations supplémentaires, nous avons supposé que la probabilité que Bob sélectionne le premier 1 / 2. Cependant, avec les informations supplémentaires que la balle choisie au hasard est rouge, cette la probabilité est passée à environ 0,645. Autrement dit, la probabilité que Bob ait sélectionné un balle de la première boîte passé de 1/ 2, quand aucune information supplémentaire était disponible, à 0,645 une fois que nous avons su que la balle sélectionnée était rouge. ▲

En utilisant le même type de raisonnement que dans l'exemple 1, nous pouvons trouver la probabilité conditionnelle qu'un événement F se produit, étant donné qu'un événement E s'est produit, lorsque l'on connaît $p(E \mid F)$, $p(E \mid \overline{F})$, et $p(F)$. Le résultat que nous pouvons obtenir est appelé **théorème de Bayes** ; il porte le nom de Thomas Bayes, un mathématicien et ministre britannique du XVIIIe siècle qui a présenté ce résultat.

THÉORÈME 1 **LE THÉORÈME DE BAYES** Supposons que E et F sont des événements d'un échantillon d'espace S tels que $p(E) = 0$ et $p(F) = 0$. Alors

$$p(F \mid E) = \frac{p(E \mid F)\, p(F)}{p(E \mid F)\, p(F) + p(E \mid F)\, p(F)}.$$

Preuve: La définition de la probabilité conditionnelle nous dit que $p(F \mid E) = p(E \cap F) / p(E)$ et $p(E \mid F) = p(E \cap F) / p(F)$. Par conséquent, $p(E \cap F) = p(F \mid E)\, p(E)$ et $p(E \cap F) = p(E \mid F)\, p(F)$. L'égalisation de ces deux expressions pour $p(E \cap F)$ montre que

$$p(F \mid E)\, p(E) = p(E \mid F)\, p(F).$$

En divisant les deux côtés par $p(E)$, nous constatons que

$$p(F \mid E) = \frac{p(E \mid F)\, p(F)}{p(E)}.$$

Ensuite, nous montrons que $p(E) = p(E \mid F)\, p(F) + p(E \mid F)\, p(F)$. Pour voir cela, première note que $E = E \cap S = E \cap (F \cup F) = (E \cap F) \cup (E \cap F)$. De plus, $E \cap F$ et $E \cap F$ sont disjoints, car si $x \in E \cap F$ et $x \in E \cap F$, alors $x \in F \cap F = \emptyset$. Par conséquent, $p(E) = p(E \cap F) + p(E \cap F)$. Nous avons déjà montré que $p(E \cap F) = p(E \mid F)\, p(F)$.
De plus, on a $p(E \mid F) = p(E \cap F) / p(F)$, ce qui montre que $p(E \cap F) = p(E \mid F)\, p(F)$. Il s'ensuit maintenant que

$$p(E) = p(E \cap F) + p(E \cap F) = p(E \mid F)\, p(F) + p(E \mid F)\, p(F).$$

Pour compléter la preuve, nous insérons cette expression pour $p(E)$ dans l'équation $p(F \mid E) = p(E \mid F)\, p(F) / p(E)$. Nous avons prouvé que

$$p(F \mid E) = \frac{p(E \mid F)\, p(F)}{p(E \mid F)\, p(F) + p(E \mid F)\, p(F)}.$$

APPLICATION DU THÉORÈME DE BAYES Le théorème de Bayes peut être utilisé pour résoudre les problèmes qui se posent dans de nombreuses disciplines. Ensuite, nous discuterons d'une application du théorème de Bayes à la médecine. Dans En particulier, nous illustrerons comment le théorème de Bayes peut être utilisé pour évaluer la probabilité que une personne testée positive pour une maladie a effectivement cette maladie. Les résultats obtenus à partir de Le théorème de Bayes est souvent quelque peu surprenant, comme le montre l'exemple 2.

EXEMPLE 2 Supposons qu'une personne sur 100 000 souffre d'une maladie rare particulière pour laquelle il existe un test de diagnostic précis. Ce test est correct 99,0% du temps lorsqu'il est administré à une personne sélectionnée au hasard qui a la maladie; il est correct 99,5% du temps lorsqu'il est donné à une personne sélectionnée au hasard qui n'a pas la maladie. Compte tenu de ces informations, pouvons-nous trouver

(a) la probabilité qu'une personne dont le test de dépistage de la maladie est positif a la maladie?

(b) la probabilité qu'une personne dont le test de dépistage de la maladie est négatif n'a pas la maladie?

Une personne dont le test est positif devrait-elle être très préoccupée par la maladie?

Solution: (a) Soit F l'événement où une personne choisie au hasard a la maladie, et soit E soit le cas où une personne choisie au hasard est positive pour la maladie. Nous voulons calculer $p(F \mid E)$. Pour utiliser le théorème de Bayes pour calculer $p(F \mid E)$, nous devons trouver $p(E \mid F)$, $p(E \mid F)$, $p(F)$ et $p(F)$.

Nous savons qu'une personne sur 100 000 a cette maladie, alors $p(F) = 1 / 100\,,000 = 0\,.\,00001$ et $p(F) = 1 - 0\,.\,00001 = 0\,.\,99999$. Parce qu'une personne atteinte de la maladie a un résultat positif à 99% le temps, on sait que $p(E \mid F) = 0\,.\,99$; c'est la probabilité d'un vrai positif, qu'une personne avec les tests de la maladie positifs. Il s'ensuit que $p(E \mid F) = 1 - p(E \mid F) = 1 - 0\,.\,99 = 0\,.\,01$; il s'agit de la probabilité d'un faux négatif, qu'une personne atteinte de la maladie soit testée négativement.

De plus, parce qu'une personne qui n'a pas le test de la maladie a un résultat négatif de 99,5% le temps, on sait que $p(E \mid F) = 0\,.\,995$. Il s'agit de la probabilité d'un vrai négatif, qu'un personne sans la maladie a un résultat négatif. Enfin, nous voyons que $p(E \mid F) = 1 - p(E \mid F) = 1 - 0\,.\,995 = 0\,.\,005$; c'est la probabilité d'un faux positif, qu'une personne sans la maladie tests positifs.

La probabilité qu'une personne dont le test est positif pour la maladie soit réellement atteinte est $p(F \mid E)$. Par le théorème de Bayes, nous savons que

$$p(F \mid E) = \frac{p(E \mid F)\, p(F)}{p(E \mid F)\, p(F) + p(E \mid F)\, p(F)}$$

$$= \frac{(0.99)(0.00001)}{(0.99)(0.00001) + (0.005)(0.99999)} \approx 0.002 .$$

(b) La probabilité qu'une personne dont le test de dépistage de la maladie est négatif n'est pas atteinte est $p(F \mid E)$. Par le théorème de Bayes, nous savons que

$$p(F \mid E) = \frac{p(E \mid F)\, p(F)}{p(E \mid F)\, p(F) + p(E \mid F)\, p(F)}$$

$$= \frac{(0.995)(0.99999)}{(0.995)(0.99999) + (0.01)(0.00001)} \approx 0.9999999 .$$

Par conséquent, 99,99999% des personnes dont le test est négatif ne souffrent vraiment pas de la maladie.

Dans la partie (a), nous avons montré que seulement 0,2% des personnes testées positives pour la maladie avoir la maladie. La maladie étant extrêmement rare, le nombre de faux positifs sur le test de diagnostic est beaucoup plus élevé que le nombre de vrais positifs, ce qui rend le pourcentage de personnes qui sont positifs et qui ont en fait une maladie extrêmement petite. Les personnes dont le test est positif les maladies ne devraient pas être trop préoccupées par le fait qu'elles ont effectivement la maladie. ▲

GÉNÉRALISER LE THÉORÈME DE BAYES Notez que dans l'énoncé du théorème de Bayes, le les événements F et F s'excluent mutuellement et couvrent tout l'espace d'échantillonnage S (c'est-à-dire $F \cup F = S$) . Nous pouvons étendre le théorème de Bayes à toute collection d'événements mutuellement exclusifs qui couvrent l'ensemble échantillonner l'espace S , de la manière suivante.

THÉORÈME 2 **Théorème des baies généralisées** Supposons que E soit un événement à partir d'un espace échantillon S et que $F_1, F_2, \ldots, F_n$ sont des événements mutuellement exclusifs tels que $\bigcup_{i=1}^{n} F_i = S$. Suppose que $p(E) = 0$ et $p(F_i) = 0$ pour $i = 1, 2, \ldots, n$. alors

$$p(F_j \mid E) = \frac{p(E \mid F_j)\, p(F_j)}{\sum_{i=1}^{n} p(E \mid F_i)\, p(F_i)} .$$

Nous laissons la preuve de cette version généralisée du théorème de Bayes à l'exercice 17.

Filtres de spam bayésiens

La plupart des boîtes aux lettres électroniques reçoivent un flot de messages indésirables et non sollicités, appelés **spam** . Étant donné que le spam menace de submerger les systèmes de courrier électronique, une un travail a été consacré à son filtrage. Certains des premiers outils développés pour éliminer le spam étaient basés sur le théorème de Bayes, tels que **les filtres anti-spam bayésiens** .

Un filtre anti-spam bayésien utilise des informations sur les messages électroniques déjà vus pour deviner si un e-mail entrant est du spam. Les filtres anti-spam bayésiens recherchent des occurrences de des mots particuliers dans les messages. Pour un mot particulier w , la probabilité que w apparaisse dans un spam le message électronique est estimé en déterminant le nombre de fois où w apparaît dans un message de un grand nombre de messages connus pour être du spam et le nombre de fois qu'il apparaît dans un grand les messages connus pour ne pas être du spam. Lorsque nous examinons les messages électroniques pour déterminer s'ils pourrait être du spam, nous examinons des mots qui pourraient être des indicateurs de spam, tels que «offre», «spécial» ou «Opportunité», ainsi que des mots qui pourraient indiquer qu'un message n'est pas du spam, comme «maman» «Déjeuner» ou «Jan» (où Jan est l'un de vos amis). Malheureusement, les filtres anti-spam échouent parfois identifier un spam comme spam; c'est ce qu'on appelle un faux négatif. Et ils identifient parfois un message qui n'est pas du spam en tant que spam; c'est ce qu'on appelle un faux positif. Lors du test de spam, il est important de minimiser les faux positifs, car le filtrage des e-mails recherchés est bien pire que laisser passer du spam.

L'utilisation du mot *spam* pour les e-mails non sollicités vient d'un Monty Croquis de comédie Python à propos d'un café où le produit alimentaire Le spam arrive avec tout indépendamment du fait que les clients le veulent.

THOMAS BAYES (1702-1761) Thomas Bayes était le fils d'un ministre d'une secte religieuse connue sous le nom de Non-conformistes. Cette secte était considérée comme hérétique dans la Grande-Bretagne du XVIIIe siècle. À cause du secret des non-conformistes, on connaît peu la vie de Thomas Bayes. Quand Thomas était jeune, sa famille a déménagé à Londres. Thomas a probablement fait ses études en privé; Les enfants non conformistes ne fréquentaient généralement pas l'école. Dans 1719 Bayes entre à l'Université d'Édimbourg, où il étudie la logique et la théologie. Il a été ordonné Ministre non conformiste comme son père et a commencé son travail en tant que ministre assistant son père. En 1733, il est devenu ministre de la Chapelle presbytérienne à Tunbridge Wells, au sud-est de Londres, où il est resté ministre jusqu'à 1752.

Bayes est surtout connu pour son essai sur la probabilité publié en 1764, trois ans après sa mort. Cet essai a été envoyé à la Royal Society par un ami qui l'a trouvé dans les papiers laissés à la mort de Bayes. dans le introduction à cet essai, Bayes a déclaré que son objectif était de trouver une méthode qui pourrait mesurer la probabilité qu'un événement se produise, en supposant que nous n'en savons rien, mais que, dans les mêmes circonstances, cela s'est produit une certaine proportion de fois. Les conclusions de Bayes ont été acceptées par le grand mathématicien français Laplace mais ont ensuite été contestées par Boole, qui a remis en question les dans son livre *Laws of Thought* . Depuis lors, les techniques de Bayes sont sujettes à controverse.

Bayes a également écrit un article publié à titre posthume: «Une introduction à la doctrine des fluxions et une défense des mathématiciens contre les objections de l'auteur de l'analyste », qui a soutenu les fondements logiques du calcul. Bayes a été élu membre de la Royal Society en 1742, avec le soutien d'importants membres de la Société, même si à cette époque fois qu'il n'avait aucun ouvrage mathématique publié. La seule publication connue de Bayes de son vivant était prétendument un livre mystique intitulé *Divine Bienveillance* , discutant de la causalité originelle et du but ultime de l'univers. Bien que le livre soit généralement attribué à Bayes, aucun nom d'auteur n'apparaissait sur la page de titre, et l'ensemble du travail serait de provenance douteuse. Les preuves des talents mathématiques de Bayes proviennent d'un cahier qui a été presque certainement écrit par Bayes, qui contient beaucoup travaux mathématiques, y compris des discussions sur les probabilités, la trigonométrie, la géométrie, les solutions d'équations, les séries et les différentiels calcul. Il y a aussi des sections sur la philosophie naturelle, dans lesquelles Bayes examine des sujets qui incluent l'électricité, l'optique et le céleste mécanique. Bayes est également l'auteur d'une publication mathématique sur les séries asymptotiques, parue après sa mort.

Nous allons développer des filtres anti-spam bayésiens de base.Tout d'abord, supposons que nous ayons un ensemble B de messages connu pour être un spam et un ensemble G de messages connus pour ne pas être du spam.(Par exemple, les utilisateurs pourraient classer les messages comme spam lorsqu'ils les examinent dans leur boîte de réception.) Nous identifions ensuite mots qui se produisent dans B et G . Nous comptons le nombre de messages dans l'ensemble contenant chacun mot pour trouver $n_B(w)$ et $n_G(w)$, le nombre de messages contenant le mot w dans les ensembles B et G , respectivement. Ensuite, la probabilité empirique qu'un message de spam contienne le mot w est $p(w) = n_B(w) / |B|$, et la probabilité empirique qu'un message qui n'est pas du spam contienne le mot w est $q(w) = n_G(w) / |G|$. On note que $p(w)$ et $q(w)$ estiment les probabilités que un message de spam entrant et un message entrant qui n'est pas du spam contiennent le mot w , respectivement.

Supposons maintenant que nous recevions un nouveau message électronique contenant le mot w . Soit S l'événement que le message est du spam. Soit E l'événement où le message contient le mot w . Les événements S , que le message est du spam, et S , que le message n'est pas du spam, partitionnez l'ensemble de tous les messages. Par conséquent, selon le théorème de Bayes, la probabilité que le message soit du spam, étant donné qu'il contient le mot w , est

$$p(S \mid E) = \frac{p(E \mid S)\, p(S)}{p(E \mid S)\, p(S) + p(E \mid S)\, p(S)}.$$

Pour appliquer cette formule, nous estimons d'abord $p(S)$, la probabilité qu'un message entrant soit spam, ainsi que $p(S)$, la probabilité que le message entrant ne soit pas du spam.Sans préalable connaissance de la probabilité qu'un message entrant soit du spam, pour simplifier nous supposons que le message est également susceptible d'être du spam qu'il ne l'est pas.Autrement dit, nous supposons que $p(S) = p(S) = 1/2$. En utilisant cette hypothèse, nous constatons que la probabilité qu'un message soit du spam, étant donné qu'il contient le mot w , est

$$p(S \mid E) = \frac{p(E \mid S)}{p(E \mid S) + p(E \mid S)}.$$

(Notez que si nous avons des données empiriques sur le rapport entre les messages de spam et les messages pas de spam, nous pouvons changer cette hypothèse pour produire une meilleure estimation de $p(S)$ et de $p(S)$; voir l'exercice 22.)

Ensuite, nous estimons $p(E \mid S)$, la probabilité conditionnelle que le message contienne le mot w étant donné que le message est du spam, par $p(w)$. De même, nous estimons $p(E \mid S)$, la con-probabilité supplémentaire que le message contienne le mot w , étant donné que le message n'est pas du spam, par $q(w)$. L'insertion de ces estimations pour $p(E \mid S)$ et $p(E \mid S)$ nous indique que $p(S \mid E)$ peut être Estimé par

$$r(w) = \frac{p(w)}{p(w) + q(w)};$$

c'est-à-dire que $r(w)$ estime la probabilité que le message soit du spam, étant donné qu'il contient le mot w . Si $r(w)$ est supérieur à un seuil que nous fixons, tel que 0.9, puis nous classons le message comme spam.

EXEMPLE 3 Supposons que nous ayons trouvé que le mot «Rolex» apparaît dans 250 des 2000 messages connus être du spam et dans 5 des 1 000 messages connus pour ne pas être du spam.Estimer la probabilité qu'un message entrant contenant le mot «Rolex» est du spam, en supposant qu'il est tout aussi probable que un message entrant est du spam ou non.Si notre seuil de rejet d'un message comme spam est 0.9, allons-nous rejeter de tels messages?

Solution: Nous utilisons le nombre de fois que le mot «Rolex» apparaît dans les messages de spam et les messages qui ne sont pas du spam pour trouver que $p(\text{Rolex}) = 250/2000 = 0.125$ et $q(\text{Rolex}) = 5/1000 = 0.005$.

Parce que nous supposons qu'il est tout aussi probable qu'un message entrant soit du spam qu'il l'est ne pas être du spam, on peut estimer la probabilité qu'un message entrant contenant le mot "Rolex" est du spam par

$$r(\text{Rolex}) = \frac{p(\text{Rolex})}{p(\text{Rolex}) + q(\text{Rolex})} = \frac{0.125}{0.125 + 0.005} = \frac{0.125}{0.130} \approx 0.962.$$

Parce que $r(\text{Rolex})$ est supérieur au seuil 0.9, nous rejetons les messages comme spam. ▲

La détection du spam sur la base de la présence d'un seul mot peut conduire à des faux positifs excessifs et les faux négatifs. Par conséquent, les filtres anti-spam vérifient la présence de plusieurs mots. Pour Par exemple, supposons que le message contienne les mots w_1 et w_2. Soit E_1 et E_2 désignent événements que le message contient les mots w_1 et w_2, respectivement. Pour faire nos calculs plus simple, nous supposons que E_1 et E_2 sont des événements indépendants et que $E_1 \mid S$ et $E_2 \mid S$ sont événements indépendants et que nous n'avons aucune connaissance préalable de savoir si le message est du spam. (Les hypothèses selon lesquelles E_1 et E_2 sont indépendantes et que $E_1 \mid S$ et $E_2 \mid S$ sont indépendant peut introduire une erreur dans nos calculs; nous supposons que cette erreur est faible.) En utilisant le théorème de Bayes et nos hypothèses, nous pouvons montrer (voir exercice 23) que $p(S \mid E_1 \cap E_2)$, la probabilité que le message soit du spam étant donné qu'il contient à la fois w_1 et w_2, est

$$p(S \mid E_1 \cap E_2) = \frac{p(E_1 \mid S)\, p(E_2 \mid S)}{p(E_1 \mid S)\, p(E_2 \mid S) + p(E_1 \mid \bar{S})\, p(E_2 \mid \bar{S})}.$$

On estime la probabilité $p(S \mid E_1 \cap E_2)$ par

$$r(w_1, w_2) = \frac{p(w_1)\, p(w_2)}{p(w_1)\, p(w_2) + q(w_1)\, q(w_2)}.$$

Autrement dit, $r(w_1, w_2)$ estime la probabilité que le message soit du spam, étant donné qu'il contient le mots w_1 et w_2. Lorsque $r(w_1, w_2)$ est supérieur à un seuil prédéfini, tel que 0.9, nous déterminons que le message est probablement du spam.

EXEMPLE 4 Supposons que nous formions un filtre anti-spam bayésien sur un ensemble de 2000 messages de spam et 1000 messages qui ne sont pas du spam. Le mot «stock» apparaît dans 400 messages de spam et 60 messages qui ne sont pas spam, et le mot «sous-évalué» apparaît dans 200 messages de spam et 25 messages qui ne sont pas Spam. Estimer la probabilité qu'un message entrant contenant à la fois les mots «stock» et «Sous-évalué» est du spam, en supposant que nous ne savons pas s'il s'agit de spam. Allons-nous rejeter ces messages comme spam lorsque nous fixons le seuil à 0.9?

Solution: utiliser le nombre de chacun de ces deux mots dans des messages connus pour être du spam ou ne pas être connu lespam, nous obtenons les estimations suivantes: $p(\text{stock}) = 400/2000 = 0.2$, $q(\text{magasin}) = 60/1000 = 0.06$, $p(\text{sous-évalué}) = 200/2000 = 0.1$, et $q(\text{sous-évalué}) = 25/1000 = 0.025$. En utilisant ces probabilités, nous pouvons estimer la probabilité que le message est du spam par

$$r(\text{stock}, \text{sous-évalué}) = \frac{p(\text{stock})\, p(\text{sous-évalué})}{p(\text{stock})\, p(\text{sous-évalué}) + q(\text{stock})\, q(\text{sous-évalué})}$$

$$= \frac{(0.2)(0.1)}{(0.2)(0.1) + (0.06)(0.025)} \approx 0.930.$$

Parce que nous avons fixé le seuil de rejet des messages à 0.9, ces messages seront rejetés par le filtre. ▲

Plus nous utilisons de mots pour estimer la probabilité qu'un message entrant soit du spam, meilleure est notre chance de déterminer correctement s'il s'agit de spam. En général, si E_i est le si le message contient le mot w_i , en supposant que le nombre de messages de spam entrants est approximativement le même que le nombre de messages entrants qui ne sont pas du spam et que événements $E_i \mid S$ sont indépendants, puis par le théorème de Bayes la probabilité qu'un message contenant tous les mots $w_1, w_2, \ldots, w_k$ est spam est

$$p\left(S \mid \bigcap_{i=1}^{k} E_i\right) = \frac{\prod_{i=1}^{k} p(E_i \mid S)}{\prod_{i=1}^{k} p(E_i \mid S) + \prod_{i=1}^{k} p(E_i \mid S)}.$$

On peut estimer cette probabilité par

$$r(w_1, w_2, \ldots, w_k) = \frac{\prod_{i=1}^{k} p(w_i)}{\prod_{i=1}^{k} p(w_i) + \prod_{i=1}^{k} q(w_i)}.$$

Pour le filtre anti-spam le plus efficace, nous choisissons des mots pour lesquels la probabilité que chacun de ces mots apparaît dans le spam est soit très élevé ou très faible.Lorsque nous calculons cette valeur pour un message particulier, nous rejetons le message comme spam si $r(w_1, w_2, \ldots, w_k)$ dépasse un préréglage seuil, tel que 0 . 9.

L'empoisonnement bayésien , le insertion de mots supplémentaires dans vaincre les filtres anti-spam, peut utiliser au hasard ou délibérément sélectionné mots.

Une autre façon d'améliorer les performances d'un filtre anti-spam bayésien consiste à examiner capacités que des paires de mots particulières apparaissent dans le spam et dans les messages qui ne le sont pasnous traiter ensuite l'apparence de ces paires de mots comme l'apparence d'un seul bloc, plutôt que comme l'apparition de deux mots distincts. Par exemple, la paire de mots «améliorer les performances» indique très probablement du spam, tandis que les «performances de l'opéra» indiquent un message qui n'est pas du spam. De même, nous pouvons évaluer la probabilité qu'un message soit du spam en examinant la structure d'un message pour déterminer où les mots y apparaissent. De plus, les filtres anti-spam examinent l'apparence de certains types de chaînes de caractères plutôt que de simples mots.Par exemple, un message avec le valide L'adresse e-mail d'un de vos amis est moins susceptible d'être du spam (si elle n'est pas envoyée par un ver) qu'une contenant une adresse e-mail provenant d'un pays connu pour être à l'origine de nombreux spams. Là est une guerre en cours entre les gens qui créent du spam et ceux qui essaient de filtrer leurs messages. Cela conduit à l'introduction de nombreuses nouvelles techniques pour vaincre les filtres anti-spam, y compris l'insertion dans les messages de spam de longues chaînes de mots qui apparaissent dans les messages qui ne sont pas du spam, ainsi que y compris des mots à l'intérieur des images. Les techniques dont nous avons discuté ici ne sont que les premières étapes dans la lutte contre cette guerre contre le spam.

Des exercices

1. Supposons que E et F sont des événements dans un espace échantillon et $p(E) = 1/3$, $P(f) = 1/2$, et $p(E \mid F) = 2/5$. Recherche $p(F \mid E)$.

2. Supposons que E et F sont des événements dans un espace échantillon et $p(E) = 2/3$, $P(f) = 3/4$, et $p(F \mid E) = 5/8$ Recherche $p(E \mid F)$.

3. Supposons que Frida sélectionne une balle en choisissant d'abord l'une des deux cases au hasard, puis en sélectionnant une balle de cette boîte au hasard. La première boîte contient deux boules blanches et trois boules bleues, et la deuxième boîte contient quatre blanches balles et une balle bleue. Quelle est la probabilité que Frida a choisi une balle de la première case si elle a sélectionné un bleu Balle?

4. Supposons qu'Ann sélectionne une balle en choisissant d'abord l'une des deux boîtes au hasard, puis en sélectionnant une balle dans cette boîte. La première boîte contient trois boules orange et quatre noires balles, et la deuxième boîte contient cinq boules orange et six boules noires. Quelle est la probabilité qu'Ann ait choisi une balle de la deuxième case si elle a sélectionné une orange Balle?

5. Supposons que 8% de tous les coureurs cyclistes utilisent des stéroïdes, un cycliste qui utilise des stéroïdes est positif pour les stéroïdes 96% du temps, et qu'un cycliste qui n'utilise pas les stéroïdes sont positifs pour les stéroïdes 9% du temps. Quoi est la probabilité qu'un cycliste choisi au hasard qui tests positifs pour les stéroïdes utilise-t-il réellement des stéroïdes?

6. Lorsqu'un test de stéroïdes est administré aux joueurs de football, 98% des joueurs prenant des stéroïdes sont positifs et 12% des les joueurs ne prenant pas de stéroïdes sont positifs. Supposons que 5% des joueurs de football prennent des stéroïdes. Quelle est la probabilité qu'un joueur de football qui teste positif prend des stéroïdes?

7. Supposons qu'un test d'utilisation de l'opium ait un faux positif de 2% et un taux de faux négatifs de 5%. Soit 2% des personnes les personnes qui n'utilisent pas de test d'opium positif pour l'opium, et

5% des utilisateurs d'opium sont négatifs pour l'opium. En outre, supposons que 1% des personnes utilisent réellement l'opium.

a) Trouvez la probabilité qu'une personne dont le test est négatif pour l'utilisation de l'opium n'utilise pas l'opium.
b) Trouver la probabilité qu'une personne dont le test est positif pour l'utilisation de l'opium utilise en fait l'opium.

8. Supposons qu'une personne sur 10 000 personnes ait une maladie génétique. Il existe un excellent test pour la maladie; 99,9% des personnes atteintes de la maladie sont positives et seulement 0,02% qui n'ont pas un test de maladie positif.

a) Quelle est la probabilité qu'une personne qui teste la positive a la maladie génétique?
b) Quelle est la probabilité qu'une personne qui teste tive n'a pas la maladie?

9. Supposons que 8% des patients testés dans une clinique soient infectés par le VIH. De plus, supposons que lorsqu'un sang test de dépistage du VIH est donné, 98% des patients infectés par Test VIH positif et que 3% des patients non infectés séropositifs. Quelle est la probabilité que

a) un patient dont le test de dépistage du VIH est positif est avec cela?
b) un patient dont le test de dépistage du VIH est positif avec ce test n'est pas infecté?
c) un patient dont le test de dépistage du VIH est négatif avec ce test est avec cela?
d) un patient dont le test de dépistage du VIH est négatif avec ce test n'est pas infecté?

10. Supposons que 4% des patients testés dans une clinique soient infectés par la grippe aviaire. De plus, supposons que lorsqu'un test sanguin pour la grippe aviaire est effectué, 97% des patients infectés par le test de l'influenza aviaire positifs et que 2% des patients non infectés par la grippe aviaire test positif. Quelle est la probabilité que

a) un patient dont le test de dépistage de la grippe aviaire est positif le test en est infecté?
b) un patient dont le test de dépistage de la grippe aviaire est positif test n'est pas infecté par elle?
c) un patient dont le test de grippe aviaire est négatif avec le test en est infecté?
d) un patient dont le test de grippe aviaire est négatif avec test n'est pas infecté par elle?

11. Une entreprise d'électronique prévoit d'introduire un nouveau téléphone appareil photo. L'entreprise commande un marketing rapport pour chaque nouveau produit qui prédit le succès ou la défaillance du produit. De nouveaux produits introduits par l'entreprise, 60% ont été des succès. En outre, 70% de leurs produits à succès devraient être succès, tandis que 40% des produits ayant échoué étaient prévus être des succès. Trouvez la probabilité que cette nouvelle caméra le téléphone réussira si son succès a été prédit.

∗ **12.** Une sonde spatiale près de Neptune communique avec la Terre des chaînes de bits. Supposons que dans ses transmissions il envoie un 1 un tiers du temps et un 0 deux tiers du temps. Lorsqu'un 0 est envoyé, la probabilité qu'il soit reçu correst de 0,9 et la probabilité qu'il soit reçu incorrectement (en tant que 1) est 0,1. Lorsqu'un 1 est envoyé, la probabilité que il est reçu correctement est de 0,8, et la probabilité qu'il soit reçu de manière incorrecte (comme un 0) est de 0,2.

a) Trouvez la probabilité qu'un 0 soit reçu.
b) Utilisez le théorème de Bayes pour trouver la probabilité qu'un a 0 a été transmis, étant donné qu'un 0 a été reçu.

13. Supposons que E , F_1 , F_2 et F_3 soient des événements d'un l'espace d'échantillon S et que F_1 , F_2 et F_3 sont disjoints sage et leur union est S . Trouver $p(F_1 \mid E)$ si $P(E \mid F_1) = 1/8$, $P(E \mid F_2) = 1/4$, $p(E \mid F_3) = 1/6$, $p(F_1) = 1/4$, $p(F_2) = 1/4$, et $p(F_3) = 1/2$.

14. Supposons que E , F_1 , F_2 et F_3 soient des événements d'un l'espace d'échantillon S et que F_1 , F_2 et F_3 sont disjoints sage et leur union est S . Trouvez $p(F_2 \mid E)$ si $p(E \mid F_1) = 2/7$, $P(E \mid F_2) = 3/8$, $P(E \mid F_3) = 1/2$, $p(F_1) = 1/6$, $p(F_2) = 1/2$, et $p(F_3) = 1/3$.

15. Dans cet exercice, nous utiliserons le théorème de Bayes pour résoudre Puzzle Monty Hall (exemple 10 dans la section 7.1). Rappel que dans ce puzzle, vous êtes invité à sélectionner l'un des trois portes à ouvrir. Il y a un gros prix derrière l'un des trois portes et les deux autres portes sont perdantes. Après Vous sélectionnez une porte, Monty Hall ouvre l'une des deux portes que vous n'a pas choisi qu'il sait être une porte perdante, sélectionnant au aléatoire si les deux perdent des portes. Monty vous demande si vous souhaitez changer de porte. Supposons que les trois les portes du puzzle sont étiquetées 1, 2 et 3. Soit W le variable aléatoire dont la valeur est le numéro du gagnant porte; supposer que $p(W = k) = 1/3$ pour $k = 1, 2, 3$. Soit M désigne la variable aléatoire dont la valeur est le nombre de la porte que Monty ouvre. Supposons que vous choisissez la porte i .

a) Quelle est la probabilité que vous gagniez le prix si le jeu se termine sans que Monty vous demande si vous vous voulez changer de porte?

b) Trouvez $p(M = j \mid W = k)$ pour $j = 1, 2, 3$ et $k = 1, 2, 3$.

c) Utilisez le théorème de Bayes pour trouver $p(W = j \mid M = k)$ où i et j et k sont des valeurs distinctes.

d) Expliquez pourquoi la réponse à la partie (c) vous indique si vous devriez changer de porte lorsque Monty vous donne le chance de le faire.

16. Ramesh peut se mettre au travail de trois manières différentes: en clé, en voiture ou en bus. En raison du trafic de banlieue, il est une chance de 50% qu'il sera en retard quand il conduira son voiture. Quand il prend le bus, qui utilise une voie spéciale servi pour les bus, il y a 20% de chances qu'il soit en retard. La probabilité qu'il soit en retard lorsqu'il chevauche son le cycle n'est que de 5%. Ramesh arrive tard un jour. Son patron veut estimer la probabilité qu'il conduise sa voiture à travailler ce jour-là.

a) Supposons que le patron suppose qu'il y a $1/3$ Risque que Ramesh prend chacune des trois façons dont il peut se rendre travail. Quelle estimation de la probabilité que Ramesh conduisait sa voiture, le patron obtient-il du théorem sous cette hypothèse?

b) Supposons que le patron sache que Ramesh conduit 30% des le temps, ne prend le bus que 10% du temps, et prend son vélo 60% du temps. Quelle estimation pour le probabilité que Ramesh conduise sa voiture fait le patron obtenir du théorème de Bayes en utilisant cette information?

∗ **17.** Prouvez le théorème 2, la forme étendue du théorem. Autrement dit, supposons que E est un événement d'un échantillon l'espace S et que $F_1, F_2, \ldots, F_n$ s'excluent mutuellement des événements tels que $\bigcup_{i=1}^{n} F_i = S$. Supposons que $p(E) \neq 0$ et $p(F_i) \neq 0$ pour $i = 1, 2, \ldots, n$. Montre CA

$$p(F_j \mid E) = \frac{p(E \mid F_j)\, p(F_j)}{\sum_{i=1}^{n} p(E \mid F_i)\, p(F_i)}.$$

[*Astuce:* utilisez le fait que $E = \bigcup_{i=1}^{n} (E \cap F_i)$.]

18. Supposons qu'un filtre anti-spam bayésien soit formé sur un ensemble de 500 messages de spam et 200 messages qui ne sont pas du spam. Le mot «passionnant» apparaît dans 40 messages de spam et dans 25 messages qui ne sont pas du spam. Un incom-être rejeté comme spam s'il contient le mot «Excitant» et le seuil de rejet du spam est 0 . 9?

19. Supposons qu'un filtre anti-spam bayésien soit formé sur un ensemble de 1000 messages de spam et 400 messages qui ne sont pas Spam. Le mot «opportunité» apparaît dans 175 messages de spam. messages et 20 messages qui ne sont pas du spam. Un message à venir soit rejeté comme spam s'il contient le mot «opportunité» et le seuil de rejet d'un message sage est 0 . 9?

20. Pourrions-nous rejeter un message comme spam dans l'exemple 4

a) en utilisant simplement le fait que le mot «sous-évalué» apparaît dans le message?

b) en utilisant simplement le fait que le mot «stock» apparaît dans le message?

21. Supposons qu'un filtre anti-spam bayésien soit formé sur un ensemble de 10 000 messages de spam et de 5 000 messages non Spam. Le mot «amélioration» apparaît dans 1500 spams messages et 20 messages qui ne sont pas du spam, tandis que le mot «à base de plantes» apparaît dans 800 messages de spam et 200 les messages qui ne sont pas du spam. Estimer la probabilité que un message reçu contenant à la fois les mots ment »et« à base de plantes »est du spam. Le message sera-t-il rejeté comme spam si le seuil de rejet du spam est 0 . 9?

22. Supposons que nous ayons des informations préalables concernant si un message entrant aléatoire est du spam. En parti-En particulier, supposons que sur une période de temps, nous trouvons que s les messages de spam arrivent et les messages h arrivent qui sont pas de spam.

a) Utilisez ces informations pour estimer $p(S)$, la probabilité un message entrant est du spam, et $p(\bar{S})$, le probabilité qu'un message entrant ne soit pas du spam.

b) Utilisez le théorème de Bayes et la partie (a) pour estimer le capacité qu'un message entrant contenant le mot w est du spam, où $p(w)$ est la probabilité que w se produise dans un message de spam et $q(w)$ est la probabilité que w se produit dans un message qui n'est pas du spam.

23. Supposons que E_1 et E_2 sont les événements qu'un entrant le message électronique contient les mots w_1 et w_2, respectivement. En supposant que E_1 et E_2 sont des événements indépendants et que $E_1 \mid S$ et $E_2 \mid S$ sont des événements indépendants, où S est le si un message entrant est du spam, et que nous avons aucune connaissance préalable quant à savoir si le message est du spam, montre que

$$p(S \mid E_1 \cap E_2) = \frac{p(E_1 \mid S)\, p(E_2 \mid S)}{p(E_1 \mid S)\, p(E_2 \mid S) + p(E_1 \mid \bar{S})\, p(E_2 \mid \bar{S})}.$$

Valeur et variance attendues

introduction

La **valeur attendue** d'une variable aléatoire est la somme de tous les éléments dans un espace échantillon du produit de la probabilité de l'élément et de la valeur de la variable aléatoire à cet élément. Par conséquent, la valeur attendue est une moyenne pondérée des valeurs d'une variable aléatoire.le La valeur attendue d'une variable aléatoire fournit un point central pour la distribution des valeurs de cette variable aléatoire. Nous pouvons résoudre de nombreux problèmes en utilisant la notion de la valeur attendue d'un variable aléatoire, telle que déterminer qui a un avantage dans les jeux de hasard et l'informatique la complexité moyenne des algorithmes. Une autre mesure utile d'une variable aléatoire est son **variance** , qui nous indique la répartition des valeurs de cette variable aléatoire.Nous pouvons utiliser le variance d'une variable aléatoire pour nous aider à estimer la probabilité qu'une variable aléatoire prenne valeurs loin de sa valeur attendue.

Valeurs attendues

De nombreuses questions peuvent être formulées en termes de valeur que nous attendons d'une variable aléatoire, ou plus précisément, la valeur moyenne d'une variable aléatoire lorsqu'une expérience est effectuée un grand nombre de fois. Les questions de ce type comprennent: Combien de têtes devraient apparaître

quand une pièce est retournée 100 fois?Quel est le nombre attendu de comparaisons utilisées pour trouver un élément dans une liste à l'aide d'une recherche linéaire? Pour étudier ces questions, nous introduisons le concept de valeur attendue d'une variable aléatoire.

DÉFINITION 1 La *valeur attendue* , également appelée *espérance* ou *moyenne* , de la variable aléatoire X sur la l'espace d'échantillon S est égal à

$$E(X) = \sum_{s \in S} p(s)\, X(s).$$

$s \in S$

L' *écart* de X à $s \in S$ est $X(s) - E(X)$, la différence entre la valeur de X et le moyenne de X .

Notez que lorsque l'espace échantillon S a n éléments $S = \{x_1, x_2, ..., x_n\}$, $E(X) = \sum_{i=1} p(x_i) X(x_i)$.

Remarque: Lorsqu'il y a une infinité d'éléments de l'espace échantillon, l'attente est dé- condamné à une amende uniquement lorsque la série infinie dans la définition est absolument convergente.En particulier, l'attente d'une variable aléatoire sur un espace échantillon infini est finie si elle existe.

EXEMPLE 1 **Valeur attendue d'un** dé Soit X le nombre qui apparaît lorsqu'un dé équitable est lancé. Quoi est la valeur attendue de X ?

Solution: La variable aléatoire X prend les valeurs 1 , 2 , 3 , 4 , 5, ou 6, chacune avec une probabilité de 1 / 6. Il s'ensuit que

$$E(X) = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \frac{1}{6} \cdot 4 + \frac{1}{6} \cdot 5 + \frac{1}{6} \cdot 6 = \frac{21}{6} = \frac{\text{sept}}{2}.$$

▲

EXEMPLE 2 Une pièce équitable est lancée trois fois. Soit S l'espace d'échantillon des huit résultats possibles, et soit X la variable aléatoire qui attribue à un résultat le nombre de têtes dans ce résultat. Quelle est la valeur attendue de X ?

Solution: dans l'exemple 10 de la section 7.2, nous avons répertorié les valeurs de X pour les huit résultats possibles lorsqu'une pièce est lancée trois fois. Parce que la pièce est juste et que les flips sont indépendants, le la probabilité de chaque résultat est de $1/8$. Par conséquent,

$$E(X) = \frac{1}{8}[X(HHH) + X(HHT) + X(HTH) + X(THH) + X(TTH) + X(THT) + X(HTT) + X(TTT)]$$

$$= \frac{1}{8}(3 + 2 + 2 + 2 + 1 + 1 + 1 + 0) = \frac{12}{8}$$

$$= \frac{3}{2}.$$

Par conséquent, le nombre attendu de têtes qui se présentent lorsqu'une pièce équitable est retournée trois fois est de 3 / deux.

▲

Lorsqu'une expérience a relativement peu de résultats, nous pouvons calculer la valeur attendue de une variable aléatoire directement à partir de sa définition, comme cela a été fait dans l'exemple 2. Cependant, quand un l'expérience a un grand nombre de résultats, il peut être gênant de calculer la valeur attendue valeur d'une variable aléatoire directement à partir de sa définition. Au lieu de cela, nous pouvons trouver la valeur attendue

d'une variable aléatoire en regroupant tous les résultats attribués la même valeur par le hasard variable, comme le montre le théorème 1.

THÉORÈME 1 Si X est une variable aléatoire et $p(X = r)$ est la probabilité que $X = r$, de sorte que $p(X = r) = \sum_{s \in S, X(s) = r} p(s)$, puis

$$E(X) = \sum_{r \in X(S)} p(X = r)\, r.$$

Preuve: Supposons que X est une variable aléatoire de gamme $X(S)$, et que $p(X = r)$ soit le proba- possibilité que la variable aléatoire X prenne la valeur r . Par conséquent, $p(X = r)$ est la somme des probabilités des résultats s tels que $X(s) = r$. Il s'ensuit que

$$E(X) = \sum_{r \in X(S)} p(X = r)\, r.$$

L'exemple 3 et la démonstration du théorème 2 illustreront l'utilisation de cette formule. Par exemple 3 nous trouverons la valeur attendue de la somme des nombres qui apparaissent sur deux dés justes lorsque ils sont roulés. Dans le théorème 2, nous trouverons la valeur attendue du nombre de succès lorsque n *Des* essais de Bernoulli sont effectués.

EXEMPLE 3 Quelle est la valeur attendue de la somme des nombres qui apparaissent quand une paire de dés équitables est roulé?

Solution: Soit X la variable aléatoire égale à la somme des nombres qui apparaissent quand un la paire de dés est lancée.Dans l'exemple 12 de la section 7.2, nous avons indiqué la valeur de X pour les 36 sorties vient de cette expérience. La plage de X est $\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Par l'exemple 12 de Section 7.2, nous voyons que

$$p(X=2)=p(X=12)=1/36,$$

$$p(X=3)=p(X=11)=2/36=1/18,$$

$$p(X=4)=p(X=10)=3/36=1/\text{douze},$$

$$p(X=5)=p(X=9)=4/36=1/9,$$

$$p(X=6)=p(X=8)=5/36,$$

$$p(X=7)=6/36=1/\text{six}.$$

En substituant ces valeurs dans la formule, nous avons

$$\begin{aligned} E(X) &= 2\cdot\frac{1}{36}+3\cdot\frac{1}{18}+4\cdot\frac{1}{12}+5\cdot\frac{1}{9}+6\cdot\frac{5}{36}+7\cdot\frac{1}{6} \\ &\quad+8\cdot\frac{5}{36}+9\cdot\frac{1}{9}+10\cdot\frac{1}{12}+11\cdot\frac{1}{18}+12\cdot\frac{1}{36} \\ &= 7. \end{aligned}$$

▲

THÉORÈME 2 Le nombre de succès escompté lorsque n essais de Bernoulli mutuellement indépendants sont formé, où p est la probabilité de réussite de chaque essai, est np.