Coleção SCHAUM

MATEMÁTICA DISCRETA

2ª edição

Seymour Lipschutz Marc Lipson

- Inclui aplicações da matemática discreta à ciência da computação
- Revisão dos temas apresentados no capítulo pela resolução dos problemas suplementares
- Cobre os conteúdos fundamentais
- Inúmeros problemas detalhadamente resolvidos

Bookman®

MAIS DE 30 MILHÕES DE EXEMPLARES VENDIDOS NO MUNDO

Coleção
SCHAUM
A essência do conhecimento

AYRES JR. & MENDELSON
Cálculo, 4.ed.

CARTER, N.
Arquitetura de Computadores

CATHEY, J.
Dispositivos e Circuitos Eletrônicos, 2.ed.

EDMINISTER, J.
Eletromagnetismo, 2.ed.

GUSTAFSON, D.
Engenharia de Software

HAYES, M.
Processamento Digital de Sinais

HSU, HWEI P.
Comunicação Analógica e Digital, 2.ed.

HSU, HWEI P.
Sinais e Sistemas

HUBBARD, J. R.
Programação em C++, 2.ed.

KAZMIER, L. J.
Estatística Aplicada à Administração e Economia, 4.ed.

LIPSCHUTZ & LIPSON
Álgebra Linear, 3.ed.

LIPSCHUTZ & LIPSON
Matemática Discreta, 2.ed.

MENDELSON, E.
Introdução ao Cálculo, 2.ed.

MOYER & AYRES JR.
Trigonometria, 3.ed.

NAHVI & EDMINISTER
Circuitos Elétricos, 4.ed.

RICH, B., revisado por P. A. SCHMIDT
Geometria, 3.ed.

ROSENBERG & EPSTEIN
Química Geral, 8.ed.

SAFIER, F.
Pré-cálculo

SCHMIDT & AYRES
Matemática para Ensino Superior, 3.ed.

SPIEGEL & LIU
Manual de Fórmulas e Tabelas Matemáticas, 2.ed.

SPIEGEL & MOYER
Álgebra, 2.ed.

SPIEGEL, SCHILLER & SRINIVASAN
Probabilidade e Estatística, 2.ed.

TITTEL, E.
Rede de Computadores

TITTEL, E.
XML

WREDE & SPIEGEL
Cálculo Avançado, 2.ed.

SEYMOUR LIPSCHUTZ, Ph.D.
Temple University

MARC LARS LIPSON, Ph.D.
University of Georgia

Teoria e Problemas de MATEMÁTICA DISCRETA

2ª Edição

Tradução:
Heloisa Bauzer Medeiros
Doutora em Matemática pela PUC-RJ
Professora adjunta IV, Instituto de Matemática, UFF

Reimpressão 2008

Bookman®

2004

Obra originalmente publicada sob o título
Schaum's Outline of Theory and Problems of Discrete Mathematics
Seymour Lipschutz, Marc Lars Lipson

ISBN 0-07-038045-7

Capa: *Rogério Grilho*

Preparação de original: *Carla Krohn*

Supervisão editorial: *Denise Weber Nowaczyk*

Editoração eletrônica: *Laser House*

SEYMOUR LIPSCHUTZ trabalha atualmente na faculdade de matemática da Temple University e lecionou anteriormente no Polytechnic Institute of Brooklyn College. Completou seu Ph.D. em 1960 no Courant Institute of Mathematical Sciences da New York University. É um dos autores mais produtivos da Coleção Schaum e escreveu também: *Probability*; *Finite Mathematics, 2nd edition*; *Álgebra Linear, 2ª edição*; *Beginning Linear Algebra; Set Theory* e *Essential Computer Mathematics*.

MARC LARS LIPSON trabalha atualmente na faculdade da University of Georgia e lecionou anteriormente na Northeastern University e Boston University. Completou seu Ph.D em 1994 na University of Michigan. Também é coautor de *2000 Solved Problems in Discrete Mathematics* com Seymour Lipschutz.

IMPRESSO NO BRASIL
PRINTED IN BRAZIL

Prefácio à segunda edição

A matemática discreta, estudo de sistemas finitos, vem assumindo importância crescente à medida que a era do computador avança. O computador é, basicamente, uma estrutura finita, e muitas das suas propriedades podem ser entendidas dentro do arcabouço formado por sistemas matemáticos finitos. Este livro, ao apresentar os conteúdos básicos, pode ser usado como livro-texto na disciplina de matemática discreta ou como um suplemento para outras matérias.

Os três primeiros capítulos tratam do conteúdo-padrão sobre conjuntos, relações e funções e algoritmos. Seguem os capítulos sobre lógica, vetores e matrizes, contagem e probabilidade. Depois, temos três capítulos sobre teoria dos grafos: grafos, grafos orientados e árvores binárias. Finalmente, capítulos avulsos tratam de propriedades dos inteiros, sistemas algébricos, linguagens e máquinas, conjuntos ordenados e reticulados e álgebra booleana. O capítulo sobre funções e algoritmos inclui uma discussão a respeito de cardinalidade e conjuntos enumeráveis e complexidade. Os capítulos que tratam de teoria dos grafos contêm discussões sobre planaridade, formas de percorrer grafos, caminhos mínimos e algoritmos de Warshall e Huffmann. O capítulo sobre linguagens e máquinas inclui expressões regulares, autômatos, máquinas de Turing e funções computáveis. Ressaltamos que os capítulos foram escritos de tal forma que a ordem pode ser alterada sem dificuldade ou perda de continuidade.

Esta segunda edição de *Matemática Discreta* supera a primeira tanto na variedade dos assuntos cobertos quanto na profundidade com que são tratados. Os tópicos em probabilidade, expressões regulares e conjuntos regulares, árvore binárias, cardinalidade, complexidade e máquinas de Turing e funções computáveis não constavam na primeira edição ou eram apenas mencionados. Este novo material reflete o fato de que matemática discreta, atualmente, é uma disciplina de um ano, e não mais de um semestre apenas.

Cada capítulo inicia com uma apresentação clara de definições pertinentes, princípios e teoremas, exemplos e outros materiais ilustrativos, seguida de conjuntos de problemas resolvidos e problemas complementares. Os problemas resolvidos visam a ilustrar e ampliar o material incluindo também demonstrações de teoremas. Os problemas complementares fornecem uma revisão completa dos temas trabalhados no capítulo. Foi incluída uma quantidade de material maior do que aquela que pode ser coberta na maioria dos cursos iniciais. O objetivo foi tornar o livro mais flexível, a fim de oferecer uma opção mais útil como referência, além de despertar interesse em outros tópicos.

Por fim, queremos agradecer à equipe da McGraw-Hill Schaum's Outline Series, especialmente a Arthur Biderman e Maureen Walker, por sua cooperação irretocável.

Seymour Lipschutz
Marc Lars Lipson

Sumário

CAPÍTULO 1 **Teoria dos Conjuntos** **11**

1.1 Introdução 11
1.2 Conjuntos e Elementos 11
1.3 Conjunto Universo e Conjunto Vazio 12
1.4 Subconjuntos 13
1.5 Diagramas de Venn 14
1.6 Operações entre Conjuntos 15
1.7 Álgebra de Conjuntos e Dualidade 17
1.8 Conjuntos Finitos, Princípio da Enumeração 19
1.9 Classes de Conjuntos, Partes de um Conjunto, Partições 20
1.10 Indução Matemática 21

CAPÍTULO 2 **Relações** **35**

2.1 Introdução 35
2.2 Produtos de Conjuntos 35
2.3 Relações 36
2.4 Representação Pictórica de Relações 37
2.5 Composição de Relações 39
2.6 Tipos de Relações 40
2.7 Propriedades de Fecho 42
2.8 Relações de equivalência 43
2.9 Relações de ordem parcial 45
2.10 Relações *n*-árias 45

CAPÍTULO 3 **Funções e Algoritmos** **56**

3.1 Introdução 56
3.2 Funções 56
3.3 Injetividade, Sobrejetividade e Funções Inversíveis 59
3.4 Funções Matemáticas, Funções Exponencial e Logaritmo 60
3.5 Seqüências, Classes Indexadas de Conjuntos 63
3.6 Funções Definidas Recursivamente 65
3.7 Cardinalidade 67
3.8 Algoritmos e Funções 68
3.9 Complexidade de Algoritmos 70

CAPÍTULO 4 **Lógica e Cálculo Proposicional** 83

4.1 Introdução 83
4.2 Proposições e Proposições Compostas 83
4.3 Operações Lógicas Básicas 84
4.4 Proposições e Tabelas-Verdade 86
4.5 Tautologias e Contradições 87
4.6 Equivalência Lógica 87
4.7 Álgebra das Proposições 88
4.8 Declarações Condicionais e Bicondicionais 89
4.9 Argumentos 89
4.10 Implicação Lógica 91
4.11 Funções Proposicionais e Quantificadores 91
4.12 Negação de Declarações com Quantificadores 94

CAPÍTULO 5 **Vetores e Matrizes** 104

5.1 Introdução 104
5.2 Vetores 105
5.3 Matrizes 107
5.4 Adição de Matrizes e Multiplicação por Escalar 107
5.5 Multiplicação de Matrizes 108
5.6 Transposta 110
5.7 Matrizes Quadradas 111
5.8 Matrizes Inversíveis (Não Singulares) e Inversas 112
5.9 Determinantes 112
5.10 Operações Elementares nas Linhas e Eliminação de Gauss (Opcional) 114
5.11 Matrizes Booleanas (Zero – Um) 119

CAPÍTULO 6 **Contagem** 135

6.1 Introdução: Princípios Básicos de Contagem 135
6.2 Notação Fatorial 136
6.3 Coeficientes Binomiais 137
6.4 Permutações 138
6.5 Combinações 140
6.6 O Princípio da Casa do Pombo 141
6.7 O Princípio de Inclusão-Exclusão 142
6.8 Partições Ordenadas e Não Ordenadas 142

CAPÍTULO 7 **Teoria das Probabilidades** 154

7.1 Introdução 154
7.2 Espaço Amostral e Eventos 154
7.3 Espaços de Probabilidade Finitos 155
7.4 Probabilidade Condicional 157
7.5 Eventos Independentes 159
7.6 Tentativas Independentes Repetidas e Distribuição Binomial 160
7.7 Variáveis Aleatórias 161

CAPÍTULO 8 **Teoria dos Grafos** 188

8.1 Introdução, Estruturas de Dados 188
8.2 Grafos e Multigrafos 190
8.3 Subgrafos, Grafos Isomorfos e Homeomorfos 192
8.4 Caminhos e Conectividade 193

8.5 As Pontes de Könisberg e Multigrafos Atravessáveis 194
8.6 Grafos Rotulados e Ponderados 196
8.7 Grafos Completos Regulares e Biparticionados 196
8.8 Árvores 198
8.9 Grafos Planares 200
8.10 Coloração de Grafos 202
8.11 Representação de Grafos na Memória de Computadores 204
8.12 Algoritmos para Grafos 206

CAPÍTULO 9 **Grafos Orientados** **229**

9.1 Introdução 229
9.2 Grafos Orientados 229
9.3 Definições Básicas 230
9.4 Árvores com Raízes 232
9.5 Representação Seqüencial de Grafos Orientados 235
9.6 Algoritmo de Warshall; Caminho Mínimo 238
9.7 Representação Ligada de Grafos Orientados 241
9.8 Algoritmos para Grafos: Buscas em Profundidade e em Largura 242
9.9 Grafos Orientados Acíclicos e Ordenação Topológica 245
9.10 Algoritmo de Poda para o Caminho Mínimo 248

CAPÍTULO 10 **Árvores Binárias** **268**

10.1 Introdução 268
10.2 Árvores Binárias 268
10.3 Árvores Binárias Completas e Estendidas 270
10.4 Representação de Árvores Binárias na Memória 272
10.5 Percorrendo Árvores Binárias 274
10.6 Árvores Binárias de Busca 276
10.7 Filas de Prioridades e *Heaps* 278
10.8 Comprimento de Caminhos e Algoritmo de Huffman 281
10.9 Árvores Gerais (Ordenadas com Raízes) Revisitadas 285

CAPÍTULO 11 **Propriedades dos Inteiros** **304**

11.1 Introdução 304
11.2 Ordem e Desigualdades, Valor Absoluto 305
11.3 Indução Matemática 306
11.4 Algoritmo de Divisão 307
11.5 Divisibilidade e Primos 309
11.6 Máximo Divisor Comum e Algoritmo de Euclides 310
11.7 Teorema Fundamental da Aritmética 312
11.8 Relação de Congruência 314
11.9 Equações de Congruência 317

CAPÍTULO 12 **Sistemas Algébricos** **349**

12.1 Introdução 349
12.2 Operações 349
12.3 Semigrupos 352
12.4 Grupos 355
12.5 Subgrupos, Subgrupos Normais e Homomorfismos 357
12.6 Anéis, Domínios Integrais e Corpos 360
12.7 Polinômios sobre um Corpo 363

CAPÍTULO 13 **Linguagens, Gramáticas e Máquinas** 387

13.1 Introdução 387
13.2 Alfabetos, Palavras e Semigrupos Livres 387
13.3 Linguagens 388
13.4 Expressões Regulares e Linguagens Regulares 389
13.5 Autômatos de Estado Finito 390
13.6 Gramáticas 393
13.7 Máquinas de Estado Finito 397
13.8 Números de Gödel 400
13.9 Máquinas de Turing 401
13.10 Funções Computáveis 404

CAPÍTULO 14 **Conjuntos Ordenados e Reticulados** 422

14.1 Introdução 422
14.2 Conjuntos Ordenados 422
14.3 Diagramas de Hasse de Conjuntos Parcialmente Ordenados 424
14.4 Enumeração Consistente 426
14.5 *Supremum* e *Infimum* 427
14.6 Conjuntos Ordenados Isomorfos (Similares) 428
14.7 Conjuntos Bem-Ordenados 429
14.8 Reticulados 431
14.9 Reticulados Limitados 433
14.10 Reticulados Distributivos 433
14.11 Complementos e Reticulados Complementados 434

CAPÍTULO 15 **Álgebra Booleana** 454

15.1 Introdução 454
15.2 Definições Básicas 454
15.3 Dualidade 455
15.4 Teoremas Básicos 456
15.5 Álgebras Booleanas como Reticulados 456
15.6 Teorema da Representação 457
15.7 Forma em Soma de Produtos para Conjuntos 458
15.8 Forma em Soma de Produtos para Álgebras Booleanas 458
15.9 Expressões Booleanas Minimais e Implicantes Primos 460
15.10 Portas Lógicas e Circuitos 463
15.11 Tabelas-Verdade e Funções Booleanas 466
15.12 Mapas de Karnaugh 468

APÊNDICE **Relações de Recorrência** 495

A.1 Introdução 495
A.2 Relações de Recorrência Lineares com Coeficientes Constantes 496
A.3 Resolução de Relações de Recorrência Lineares Homogêneas 498
A.4 Resolução de Relações Lineares de Recorrência Genéricas 500

ÍNDICE 505

Capítulo 1

Teoria dos Conjuntos

1.1 INTRODUÇÃO

O conceito de *conjunto* está presente em toda a matemática. Este capítulo apresenta a notação e a terminologia da teoria dos conjuntos, que é um assunto básico e será usado no decorrer do texto.

Apesar de o estudo de lógica ser formalmente tratado no Capítulo 4, apresentamos aqui a representação de conjuntos por diagramas de Venn e mostramos sua aplicação para argumentos lógicos. A relação entre a teoria dos conjuntos e a lógica será explorada posteriormente na discussão sobre álgebra booleana no Capítulo 15.

Este capítulo se encerra com a definição formal de indução matemática com exemplos.

1.2 CONJUNTOS E ELEMENTOS

Um *conjunto* pode ser considerado como uma coleção de objetos, os *elementos* ou *membros* do conjunto. Normalmente usamos letras maiúsculas, $A, B, X, Y, \ldots$, para denotar conjuntos, e letras minúsculas, $a, b, x, y, \ldots$, para denotar elementos de conjuntos. A afirmação "p é um elemento de A" ou, equivalentemente, "p pertence a A", é escrita

$$p \in A$$

A afirmação de que p não é um elemento de A, isto é, a negação de $p \in A$, é escrita

$$p \notin A$$

O fato de que um conjunto fica completamente determinado quando seus elementos são especificados é formalmente conhecido como princípio da extensão.

Princípio da extensão: Dois conjuntos, A e B, são iguais se e somente se possuem os mesmos elementos.

Como de hábito, escrevemos $A = B$ se os conjuntos A e B são iguais, e escrevemos $A \neq B$ se os conjuntos não são iguais.

Descrição de Conjuntos

Existem essencialmente duas maneiras de especificar um conjunto particular. Uma opção, quando possível, consiste em listar seus elementos. Por exemplo,

$$A = \{a, e, i, o, u\}$$

denota o conjunto A cujos elementos são as letras a, e, i, o, u. Observe que os elementos são separados por vírgulas e se encontram dentro de chaves { }.

A segunda maneira consiste em enunciar as propriedades que caracterizam os elementos do conjunto. Por exemplo:

$$B = \{x: x \text{ é um inteiro par}, x > 0\},$$

que deve ser lido como "B é o conjunto dos x tal que x é um inteiro par e x é maior do que 0", significa que os elementos do conjunto B são os inteiros positivos. Uma letra, usualmente x, é usada para designar um elemento típico do conjunto; dois-pontos é lido como "tal que", e a vírgula como "e".

Exemplo 1.1

(*a*) O conjunto A definido anteriormente também pode ser escrito como:

$$A = \{x: x \text{ é uma letra do alfabeto}, x \text{ é uma vogal}\}$$

Observe que $b \notin A$, $e \in A$ e $p \notin A$.

(*b*) Não seria possível listar todos elementos do conjunto B acima, embora freqüentemente se possa especificar o conjunto escrevendo

$$B = \{2, 4, 6, \ldots\},$$

onde se assume que o significado da especificação pode ser entendido por todos. Observe que $8 \in B$, mas $-7 \notin B$.

(*c*) Seja $E = \{ x : x^2 - 3x + 2 = 0 \}$. Em outras palavras, E é o conjunto das soluções da equação $x^2 - 3x + 2 = 0$, por vezes denominado o *conjunto solução* da equação. Como as soluções da equação são 1 e 2, poderíamos também escrever $E = \{1, 2\}$.

(*d*) Seja $E = \{ x : x^2 - 3x + 2 = 0 \}$, $F = \{ 2, 1 \}$ e $G = \{ 1, 2, 2, 1, 6/3 \}$. Então $E = F = G$. Observe que um conjunto não depende da maneira como seus elementos são representados. Um conjunto não se altera se os elementos são repetidos ou reordenados.

Alguns conjuntos vão aparecer com muita freqüência no texto e, por esta razão, usaremos símbolos especiais para representá-los. A menos de especificação em contrário, vamos considerar o seguinte:

$\mathbf{N}$ = o conjunto de inteiros positivos: 1, 2, 3, ...,
$\mathbf{Z}$ = o conjunto dos inteiros: ..., –2, –1, 0, 1, 2 ...,
$\mathbf{Q}$ = o conjunto dos números racionais,
$\mathbf{R}$ = o conjunto dos números reais,
$\mathbf{C}$ = o conjunto dos números complexos.

Mesmo quando for possível listar os elementos de determinado conjunto, pode não ser muito prático fazê-lo. Por exemplo, não listaríamos os elementos do conjunto das pessoas nascidas no mundo durante o ano de 1976 embora, teoricamente, seja possível compilar essa lista. Isto é, descrevemos um conjunto listando seus elementos apenas se o número desses elementos for pequeno; caso contrário, descrevemos o conjunto pela propriedade que caracteriza seus elementos.

O fato de que um conjunto pode ser descrito em função de uma propriedade é formalmente conhecido como *princípio da abstração*.

Princípio da abstração: Dado um conjunto U e uma propriedade P, existe um conjunto A tal que os elementos de A são os elementos de U que possuem a propriedade P.

1.3 CONJUNTO UNIVERSO E CONJUNTO VAZIO

Em qualquer aplicação da teoria dos conjuntos, os elementos de todos conjuntos considerados pertencem a algum conjunto maior, conhecido como *conjunto universo*. Por exemplo, em geometria plana, o conjunto universo compõe-se de todos os pontos do plano e, em estudos de populações humanas, o conjunto universo compõe-se de todas as pessoas do mundo. Vamos usar o símbolo

$$U$$

para denotar o conjunto universo, a menos que se mencione explicitamente, ou esteja implícito no contexto, um significado diferente para o símbolo.

Para um dado conjunto U e uma propriedade P, é possível que não existam elementos em U satisfazendo a propriedade P. Por exemplo, o conjunto

$$S = \{x: x \text{ é um inteiro positivo}, x^2 = 3\}$$

não possui elementos, já que nenhum inteiro positivo tem a propriedade requerida.

O conjunto que não contém elementos é chamado de *conjunto vazio*[†] e é denotado por:

$$\varnothing$$

Existe apenas um conjunto vazio. Isto é: se S e T são vazios, então $S = T$, já que possuem exatamente os mesmos elementos, isto é, nenhum.

1.4 SUBCONJUNTOS

Se todo elemento de um conjunto A é também um elemento de um conjunto B, diz-se que A é um *subconjunto* de B. Também dizemos que A está *contido* em B ou que B *contém* A. Essa relação é escrita como segue:

$$A \subseteq B \text{ ou } B \supseteq A$$

Se A não é um subconjunto de B, isto é, se pelo menos um elemento de A não pertence a B, escrevemos $A \nsubseteq B$ ou $B \not\supseteq A$.

Exemplo 1.2

(*a*) Considere os conjuntos

$$A = \{1, 3, 4, 5, 8, 9\} \qquad B = \{1, 2, 3, 5, 7\} \qquad C = \{1, 5\}$$

Então, $C \subseteq A$ e $C \subseteq B$, já que 1 e 5, os elementos de C, são também elementos de A e B. Mas $B \nsubseteq A$, uma vez que seus elementos, por exemplo, 2 e 7, não pertencem a A. Além disso, como os elementos de A, B e C também devem pertencer ao conjunto universo U, concluímos que U deve, pelo menos, conter o conjunto {1, 2, 3, 4, 5, 6, 7, 8, 9}.

(*b*) Sejam **N**, **Z**, **Q** e **R** definidos como na Seção 1.2. Então:

$$\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

(*c*) O conjunto $E = \{2, 4, 6\}$ é um subconjunto do conjunto $F = \{6, 2, 4\}$, já que cada um dos elementos 2, 4 e 6 pertencentes a E também pertencem a F. Na verdade, $E = F$. De maneira análoga, é possível mostrar que todo conjunto é um subconjunto de si mesmo.

As seguintes propriedades de conjuntos devem ser observadas:

(i) Todo conjunto A é um subconjunto do conjunto universo, já que, por definição, todos elementos de A pertencem U. O conjunto vazio, $\varnothing$, também é um subconjunto de A.

(ii) Todo conjunto A é um subconjunto de si mesmo, uma vez que, trivialmente, os elementos de A pertencem a A.

(iii) Se todo elemento de A pertence a um conjunto B, e todo elemento de B pertence a um conjunto C, então claramente todo elemento de A pertence a C. Em outras palavras, se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(iv) Se $A \subseteq B$ e $B \subseteq A$, então A e B têm os mesmos elementos, i. e., $A = B$. Por outro lado, se $A = B$, então $A \subseteq B$ e $B \subseteq A$, já que todo elemento é um subconjunto de si mesmo.

Enunciamos esses resultados formalmente no teorema a seguir.

Teorema 1-1: (i) Para todo conjunto A, temos $\varnothing \subseteq A \subseteq U$.

(ii) Para todo conjunto A, $A \subseteq A$.

(iii) Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(iv) $A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$.

Se $A \subseteq B$, é possível que $A = B$. Quando $A \subseteq B$ mas $A \neq B$, dizemos que A é um *subconjunto próprio* de B. Escreveremos $A \subset B$ quando A é um subconjunto próprio de B. Por exemplo, suponha

$$A = \{1, 3\} \qquad B = \{1, 2, 3\}, \qquad C = \{1, 3, 2\}.$$

Então, A e B são subconjuntos de C; mas A é um subconjunto próprio de C, enquanto B não é um subconjunto próprio de C, já que $B = C$.

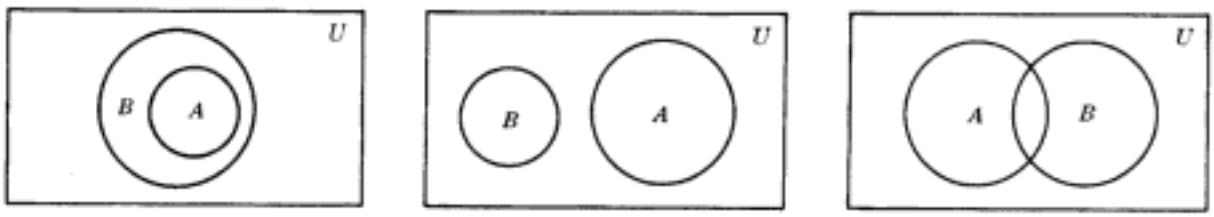
[†] N. de T. No original, *empty set* ou *null set*.

1.5 DIAGRAMAS DE VENN

Um diagrama de Venn é uma representação pictórica na qual os conjuntos são representados por áreas delimitadas por curvas no plano.

O conjunto universo U é representado pelo interior de um retângulo, e os outros conjuntos, por discos contidos dentro desse retângulo. Se $A \subseteq B$, o disco que representa A deve estar inteiramente contido no disco que representa B como na Fig. 1-1(a). Se A e B são disjuntos, i. e., se eles não possuem elementos em comum, então o disco representando A estará separado do disco representando B como na Figura 1-1(b).

Entretanto, se A e B são dois conjuntos arbitrários, é possível que alguns objetos estejam em A mas não em B, alguns estejam em B mas não em A, alguns estejam em ambos e alguns não estejam nem em A nem em B; portanto, em geral representamos A e B como na Figura 1-1 (c).



(a) $A \subseteq B$ (b) A e B são disjuntos (c)

Fig. 1-1

Argumentos e Diagramas de Venn

Muitas afirmativas feitas verbalmente são essencialmente afirmativas sobre conjuntos e podem, portanto, ser descritas através de diagramas de Venn.

Logo, os diagramas de Venn podem ser usados para determinar se um argumento é ou não válido. Considere o exemplo seguinte.

Exemplo 1.3 Mostre que o seguinte argumento (adaptado de um livro de lógica de Lewis Carroll, autor de *Alice no País das Maravilhas*) é válido:

S_1: Minhas panelas são os únicos objetos feitos de metal que possuo.
S_2: Eu acho todos os seus presentes muito úteis.
S_3: Nenhuma das minhas panelas é de pouca utilidade.

S: Seus presentes para mim não são feitos de metal.

(As afirmativas S_1, S_2 e S_3 são as hipóteses, e a afirmação S é a conclusão. O argumento é válido se a conclusão S segue logicamente das hipóteses S_1, S_2 e S_3.)

Por S_1 os objetos de metal estão contidos no conjunto de panelas e, por S_3, o conjunto de panelas e o conjunto de objetos úteis são distintos; logo, desenhamos o diagrama de Venn (Figura 1-2).

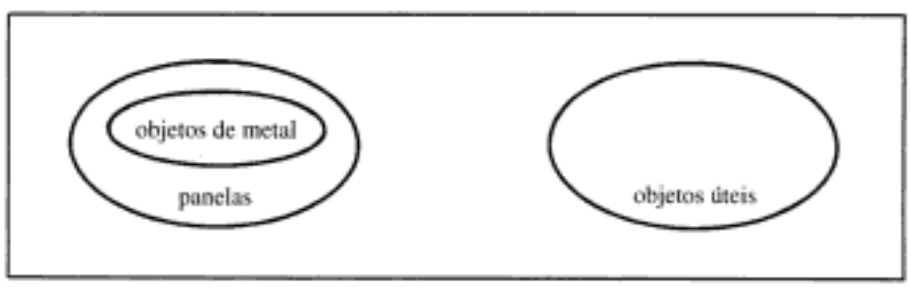


Fig. 1-2

Por S_2, o conjunto "seus presentes" é um subconjunto do conjunto dos objetos úteis e, portanto, desenhamos como está representado na Figura 1-3.

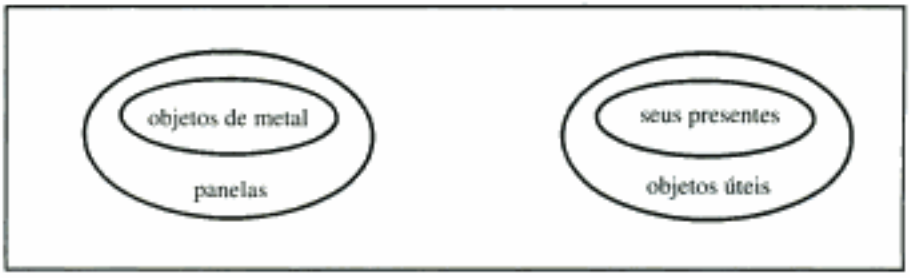


Fig. 1-3

A conclusão é claramente válida de acordo com o diagrama de Venn acima porque o conjunto "seus presentes " é disjunto do conjunto de objetos de metal.

1.6 OPERAÇÕES ENTRE CONJUNTOS

Esta seção apresenta várias operações importantes entre conjuntos.

União e Interseção

A *união* de dois conjuntos A e B, denotada por $A \cup B$, é o conjunto de todos elementos que pertencem a A ou a B; isto é:

$$A \cup B = \{x: x \in A \text{ ou } x \in B\}$$

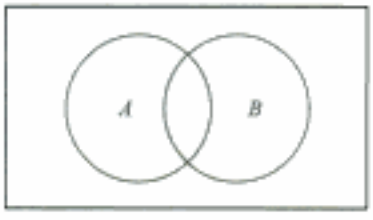
Aqui "ou" é usado no sentido de e/ou. A Figura 1-4(a) é um diagrama de Venn no qual $A \cup B$ está sombreado.

A *interseção* de dois conjuntos A e B, denotada por $A \cap B$, é o conjunto dos elementos que pertencem a A e a B; isto é,

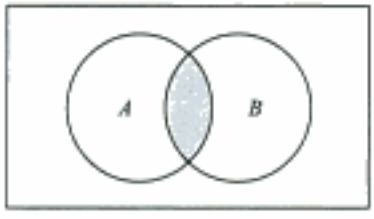
$$A \cap B = \{x: x \in A \text{ e } x \in B\}$$

A Figura 1-4(b) é um diagrama de Venn no qual $A \cap B$ está sombreado.

Se $A \cap B = \varnothing$, isto é, se A e B não possuem elementos em comum, então A e B são ditos *disjuntos*.



(a) $A \cup B$ está sombreado



(b) $A \cap B$ está sombreado

Fig. 1-4

Exemplo 1.4

(a) Seja $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, $C = \{2, 3, 5, 7\}$. Então,

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\} \qquad A \cap B = \{3, 4\}$$
$$A \cup C = \{1, 2, 3, 4, 5, 7\} \qquad A \cap C = \{2, 3\}$$

(b) Suponha que M denota o conjunto de estudantes do sexo masculino de uma universidade C, e F denota o conjunto de estudantes do sexo feminino na universidade C. Então,

$$M \cup F = C$$

já que cada estudante de C pertence a apenas um dos conjuntos, M ou F. Por outro lado,

$$M \cap F = \varnothing$$

já que nenhum estudante pertence a ambos os conjuntos M e F.

A operação de inclusão de conjuntos está intimamente relacionada às operações de união e interseção, como demonstra o teorema a seguir.

Teorema 1-2: são equivalentes $A \subseteq B$, $A \cap B = A$ e $A \cup B = B$.

Nota: Esse teorema está demonstrado no Problema 1.27. Outras condições equivalentes a $A \subseteq B$ são apresentadas no Problema 1.37.

Complementares

Lembramos que todos conjuntos considerados em cada situação são subconjuntos de um conjunto universo fixo, U. O *complementar absoluto*, ou simplesmente *complementar de um conjunto* A, denotado por A^C, é o conjunto dos elementos que pertencem a U mas não pertencem a A; isto é,

$$A^c = \{x: x \in U, x \notin A\}$$

Alguns textos utilizam a notação A' ou $\bar{A}$ para o complementar de A. A Figura 1-5(a) é um diagrama de Venn em que A^C está sombreado.

O *complementar relativo* de um conjunto B em relação a A, ou simplesmente a diferença entre A e B, denotado por $A\backslash B$, é o conjunto dos elementos que pertencem a A mas não pertencem a B, isto é,

$$A\backslash B = \{x: x \in A, x \notin B\}$$

O conjunto $A\backslash B$ é chamado de "A menos B". Muitos textos denotam $A\backslash B$ por $A - B$ ou por $A \sim B$. A Figura 1-5(b) é um diagrama de Venn onde $A\backslash B$ está sombreado.

(a) A^C está sombreado (b) $A\backslash B$ está sombreado

Fig. 1-5

Exemplo 1.5 Suponha que $U = \mathbf{N} = \{1, 2, 3, \ldots\}$, o conjunto de inteiros positivos, seja o conjunto universo. Sejam

$$A = \{1, 2, 3, 4, \}, \qquad B = \{3, 4, 5, 6, 7\}, \qquad C = \{6, 7, 8, 9\},$$

e seja $E = \{2, 4, 6, 8, \ldots\}$, os inteiros pares. Então,

$$A^c = \{5, 6, 7, 8, \ldots\}, \qquad B^c = \{1, 2, 8, 9, 10, \ldots\}, \qquad C^c = \{1, 2, 3, 4, 5, 10, 11, \ldots\}$$

e

$$A\backslash B = \{1, 2\}, \qquad B\backslash C = \{3, 4, 5\}, \qquad B\backslash A = \{5, 6, 7\}, \qquad C\backslash E = \{7, 9\}.$$

Além disso, $E^C = \{1, 3, 5, \ldots\}$, o conjunto dos inteiros ímpares.

Produtos Fundamentais

Considere n conjuntos distintos $A_1, A_2, \ldots, A_n$. Um produto fundamental de conjuntos é um conjunto da forma

$$A_1^* \cap A_2^* \cap \cdots \cap A_n^*,$$

onde A_i^* pode representar A_i ou A_i^c. Observamos que (1) existem 2^n produtos fundamentais, (2) quaisquer dois produtos fundamentais são disjuntos, e (3) o conjunto universo U é a união de todos os produtos fundamentais (Problema 1.64). Há uma descrição geométrica desses conjuntos que está ilustrada na próxima página.

Exemplo 1.6 Considere três conjuntos, A, B C. Estão listados a seguir os oito produtos fundamentais dos três conjuntos.

$$P_1 = A \cap B \cap C, \qquad P_3 = A \cap B^c \cap C, \qquad P_5 = A^c \cap B \cap C, \qquad P_7 = A^c \cap B^c \cap C$$
$$P_2 = A \cap B \cap C^c \qquad P_4 = A \cap B^c \cap C^c, \qquad P_6 = A^c \cap B \cap C^c \qquad P_8 = A^c \cap B^c \cap C^c$$

Esses oito produtos correspondem precisamente às oito regiões assinaladas nos diagramas de Venn de A, B, C da Figura 1.6 como indicado nas regiões identificadas.

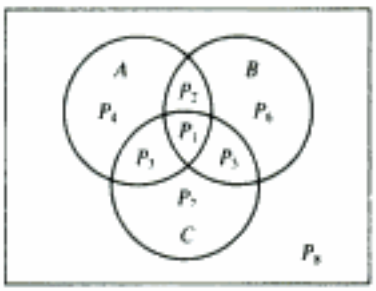
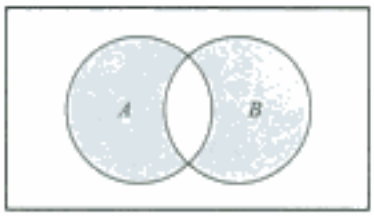


Fig. 1-6



A ⊕ B está sombreado

Fig. 1-7

Diferença Simétrica

A *diferença simétrica* dos conjuntos A e B, denotada por $A \oplus B$, consiste em todos os elementos que pertencem a A ou a B mas não a ambos; isto é,

$$A \oplus B = (A \cup B) \backslash (A \cap B)$$

É possível mostrar (Problema 1.18) que

$$A \oplus B = (A \backslash B) \cup (B \backslash A)$$

Por exemplo, suponha $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{4, 5, 6, 7, 8, 9\}$. Então:

$$A \backslash B = \{1, 2, 3\}, \qquad B \backslash A = \{7, 8, 9\} \qquad \text{e, portanto,} \qquad A \oplus B = \{1, 2, 3, 7, 8, 9\}$$

A Figura 1-7 é um diagrama de Venn no qual $A \oplus B$ está sombreado.

1.7 ÁLGEBRA DE CONJUNTOS E DUALIDADE

Conjuntos munidos das operações de união, interseção e determinação de complementar[†] satisfazem a várias leis ou identidades que estão listadas na Tabela 1-1. Na verdade, afirmamos formalmente o seguinte:

Teorema 1-3: os conjuntos satisfazem as leis na Tabela 1-1.

Existem dois métodos de demonstrar equações que envolvem operações entre conjuntos. Uma maneira é usar as propriedades requeridas para que um elemento x satisfaça cada lado da igualdade, e a outra é usar diagramas de Venn. Por exemplo, considere a primeira lei de DeMorgan,

$$(A \cup B)^c = A^c \cap B^c$$

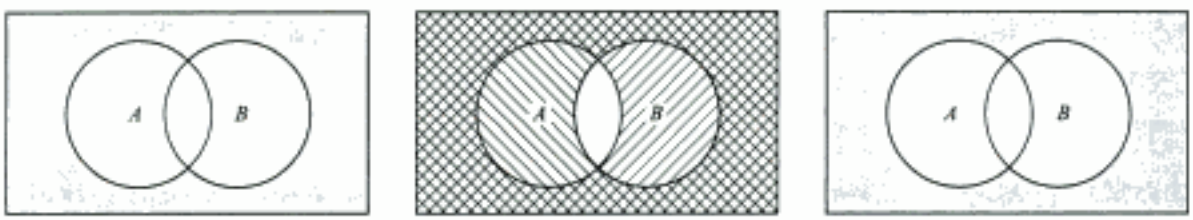
[†] N. de T. *Complements, em inglês.*

Tabela 1-1 Leis da álgebra de conjuntos

Leis de idempotência	
(1a) $A \cup A = A$	(1b) $A \cap A = A$
Leis de associatividade	
(2a) $(A \cup B) \cup C = A \cup (B \cup C)$	(2b) $(A \cap B) \cap C = A \cap (B \cap C)$
Leis de comutatividade	
(3a) $A \cup B = B \cup A$	(3b) $A \cap B = B \cap A$
Leis de distributividade	
(4a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(4b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Leis de identidade	
(5a) $A \cup \varnothing = A$	(5b) $A \cap U = A$
(6a) $A \cup U = U$	(6b) $A \cap \varnothing = \varnothing$
Leis de involução	
(7) $(A^c)^c = A$	
Leis dos complementares[†]	
(8a) $A \cup A^c = U$	(8b) $A \cap A^c = \varnothing$
(9a) $U^c = \varnothing$	(9b) $\varnothing^c = U$
Leis de DeMorgan	
(10a) $(A \cup B)^c = A^c \cap B^c$	(10b) $(A \cap B)^c = A^c \cup B^c$

Método 1: Mostramos primeiramente que $(A \cup B)^c \subseteq A^c \cap B^c$. Se $x \in (A \cup B)^c$, então $x \notin A \cup B$. Logo, $x \notin A$ e $x \notin B$, portanto $x \in A^c$ e $x \in B^c$.
Assim, $x \in A^c \cap B^c$. A seguir, mostramos que $A^c \cap B^c \subseteq (A \cup B)^c$. Seja $x \in A^c \cap B^c$. Então, $x \in A^c$ e $x \in B^c$; logo, $x \notin A$ e $x \notin B$. Portanto, $x \notin A \cup B$, e logo $x \in (A \cup B)^c$.
Mostramos que todo elemento de $(A \cup B)^c$ pertence a $A^c \cap B^c$ e que todo elemento de $A^c \cap B^c$ pertence a $(A \cup B)^c$. Essas duas inclusões, consideradas conjuntamente, mostram que os conjuntos têm os mesmos elementos, i. e., que $(A \cup B)^c = A^c \cap B^c$.

Método 2: Pelo diagrama de Venn para $A \cup B$ na Fig. 1-4, vemos que $(A \cup B)^c$ é representado pela área sombreada na Fig.1-8(*a*). Para achar $A^c \cap B^c$, isto é, a área em A^c e B^c, tracejamos A^c em uma direção e A^B em outra como na Fig. 1-8(*b*). Então, $A^c \cap B^c$ é representado pela área com tracejado nos dois sentidos, sombreada na Fig. 1-8(*c*). Como $(A \cup B)^c$ e $A^c \cap B^c$ são representados pela mesma área, eles são iguais.



(*a*) $(A \cup B)^c$ está sombreado

(*b*) A^c está sombreado com ////
B^c está sombreado com \\\\

(*c*) $A^c \cap B^c$ está sombreado

Fig. 1-8

Dualidade

Observe que as identidades na Tabela 1-1 estão organizadas em pares, como, por exemplo, (2*a*) e (2*b*). Trataremos agora do princípio envolvido nessa organização. Suponha que E seja uma equação da álgebra de conjuntos. A equação dual de E, E^*, é a equação obtida pela substituição de cada ocorrência de $\cup$, $\cap$, U e $\varnothing$ em E por, respectivamente, $\cap$, $\cup$, $\varnothing$ e U. Por exemplo, o dual de

[†] N. de T. No original, *complement Laws*.

$$(U \cap A) \cup (B \cap A) = A \qquad \text{é} \qquad (\varnothing \cup A) \cap (B \cup A) = A$$

Observe que cada par de leis na Tabela 1-1 é composto de equações duais uma da outra. É um fato na álgebra de conjuntos que, se uma equação E for uma identidade, sua dual, E^*, também é uma identidade.

1.8 CONJUNTOS FINITOS, PRINCÍPIO DA ENUMERAÇÃO

Um conjunto é dito finito se contém exatamente m elementos distintos, onde m denota algum inteiro não negativo. Caso contrário, o conjunto é dito infinito. Por exemplo, o conjunto vazio, $\varnothing$, e o conjunto de letras do alfabeto são conjuntos finitos, enquanto o conjunto de inteiros positivos pares, $\{2, 4, 6, \ldots\}$, é infinito.

A notação $n(A)$ será usada para denotar o número de elementos de um conjunto finito A[†]. Alguns textos usam $\#(A)$, $|A|$ ou card(A) em vez de $n(A)$.

Lema 1-4: se A e B são conjuntos finitos disjuntos, então $A \cup B$ é finito e

$$n(A \cup B) = n(A) + n(B).$$

Ao contar os elementos de $A \cup B$, primeiramente conte os que estão em A. Existem $n(A)$ elementos em A. Os únicos outros elementos de $A \cup B$ são aqueles que estão em B, mas não em A. Mas como A e B são disjuntos, nenhum elemento de B está em A e, portanto, existem $n(B)$ elementos que estão em B mas não estão em A. Logo, $n(A \cup B) = n(A) + n(B)$.

Há também uma fórmula para $n(A \cup B)$ mesmo quando os conjuntos não são disjuntos. Esse fato é demonstrado no Problema 1.28.

Teorema 1-5: se A e B são conjuntos finitos, então $A \cup B$ e $A \cap B$ são finitos e

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Podemos aplicar esse resultado para obter uma fórmula similar para três conjuntos:

Corolário 1-6: se A, B e C são conjuntos finitos, então $A \cup B \cup C$ também é, e

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C).$$

Pode-se usar indução matemática (Seção 1.10) para generalizar esse resultado para qualquer número finito de conjuntos.

Exemplo 1.7 Considere os seguintes dados sobre 120 estudantes de matemática no que diz respeito aos idiomas francês, alemão e russo.

65 estudam francês,
45 estudam alemão,
42 estudam russo,
20 estudam francês e alemão,
25 estudam francês e russo,
15 estudam alemão e russo,
8 estudam os três idiomas.

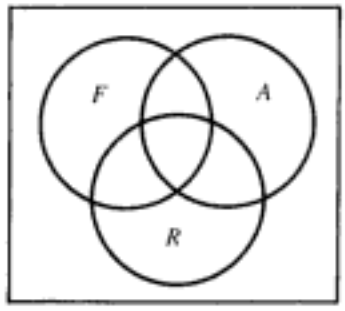


Fig. 1-9

Sejam F, A e R os conjuntos de alunos que estudam francês, alemão e russo, respectivamente. Queremos determinar o número de alunos que estudam pelo menos um dos três idiomas e preencher o diagrama de Venn da Figura 1-9 com o número correto de estudantes em cada região.

Pelo Corolário 1-6,

$$\begin{aligned} n(F \cup A \cup R) &= n(F) + n(A) + n(R) - n(F \cap A) - n(F \cap R) - n(A \cap R) + n(F \cap A \cap R) \\ &= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100 \end{aligned}$$

[†] N. de T. O termo mais usado em português para número de elementos de um conjunto A é cardinalidade de A.

Isto é, $n(F \cup A \cup R) = 100$ alunos estudam pelo menos um dos três idiomas.

Usamos então esse resultado para preencher o diagrama de Venn. Temos:

8 estudam os três idiomas;
$20 - 8 = 12$ estudam francês e alemão, mas não russo;
$25 - 8 = 17$ estudam francês e russo, mas não alemão;
$15 - 8 = 7$ estudam alemão e russo, mas não francês;
$65 - 12 - 8 - 17 = 28$ estudam apenas francês;
$45 - 12 - 8 - 7 = 18$ estudam apenas alemão;
$42 - 17 - 8 - 7 = 10$ estudam apenas francês;
$120 - 100 = 20$ não estudam idioma algum.

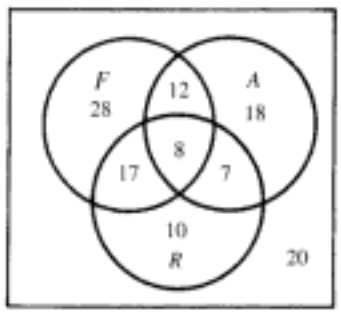


Fig. 1-10

O diagrama completo aparece na Figura 1-10. Observe que $28 + 18 + 10 = 56$ alunos estudam apenas um idioma.

1.9 CLASSES DE CONJUNTOS, PARTES DE UM CONJUNTO, PARTIÇÕES

Dado um conjunto S, podemos querer tratar de alguns dos seus subconjuntos. Neste caso, estaríamos considerando um conjunto de subconjuntos. Sempre que uma situação dessas ocorrer, a fim de evitar mal-entendidos, vamos nos referir a uma *classe* de conjuntos ou *coleção* de conjuntos no lugar de um conjunto de conjuntos. Se desejarmos considerar alguns dos conjuntos de uma determinada classe, falaremos de uma *subclasse* ou uma *subcoleção*.

Exemplo 1.8 Suponha que $S = \{1, 2, 3, 4\}$. Seja $\mathcal{A}$ a classe de subconjuntos de S que contêm exatamente três elementos de S. Então,

$$\mathcal{A} = [\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}]$$

Os elementos de $\mathcal{A}$ são os conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1,3, 4\}$ e $\{2, 3, 4\}$.
Seja $\mathcal{B}$ a classe dos subconjuntos de S que contêm o número 2 e outros dois elementos de S. Então,

$$\mathcal{B} = [\{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}].$$

Os elementos de $\mathcal{B}$ são os conjuntos $\{1, 2, 3\}$, $\{1, 2, 4\}$ e $\{2, 3, 4\}$. Portanto, $\mathcal{B}$ é uma subclasse de $\mathcal{A}$, já que todo elemento de $\mathcal{B}$ é também um elemento de $\mathcal{A}$. (Para evitar confusões, vamos por vezes usar colchetes em vez de parênteses para indicar conjuntos de uma mesma classe.)

Partes de um Conjunto[†]

Para um dado conjunto S, podemos falar do conjunto de todos os subconjuntos de S. Essa classe é chamada de conjunto das *partes* de S e será denotada por Partes(S). Se S é finito, então Partes(S) também é. Na verdade, o número de elementos de Partes(S) é 2 elevado à cardinalidade de S; isto é,

$$n(\text{Partes}(S)) = 2^{n(S)}$$

(Por esta razão, o conjunto das partes de S é geralmente denotado por 2^S.)

Exemplo 1-9 Suponha que $S = \{1, 2, 3\}$. Então,

$$\text{Partes}(S) = [\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S].$$

Observe que o conjunto $\varnothing$ pertence a Partes(S), pois $\varnothing$ é um subconjunto de S. De maneira similar, S pertence a Partes(S). Como era de se esperar da observação acima, Partes(S) tem $2^3 = 8$ elementos.

Partições

Seja S um conjunto não vazio. Uma partição de S é uma subdivisão de S em conjuntos não vazios disjuntos. Mais precisamente, uma *partição* de S é uma coleção $\{ A_i \}$ de subconjuntos não vazios de S tais que:

(i) Cada a em S pertence a algum dos A_i.
(ii) Os conjunto em $\{ A_i \}$ são disjuntos dois a dois; isto é, se

[†] N. de T. Em inglês, *power sets*, usualmente traduzido como o conjunto de todos os subconjuntos de um conjunto, ou o conjunto das partes de um conjunto.

$$A_i \neq A_j, \quad \text{então} \quad A_i \cap A_j = \varnothing$$

Os subconjuntos de uma partição são chamados de *células*. A Figura 1-11 apresenta um diagrama de Venn de uma partição de um conjunto de pontos retangular S em cinco células A_1, A_2, A_3, A_4 e A_5.

Exemplo 1.10 Considere a seguinte coleção de subconjuntos de $S = \{1, 2, \ldots, 8, 9\}$:

(i) $[\{1,3,5\}, \{2,6\}, \{4,8,9\}]$
(ii) $[\{1,3,5\}, \{2,4,6,8\}, \{5,7,9\}]$
(iii) $[\{1,3,5\}, \{2,4,6,8\}, \{7,9\}]$

Então (i) não é uma partição de S, pois 7 pertence a S e não está em nenhum dos subconjuntos. Além do mais, (ii) não é uma partição de S, já que $\{1, 3, 5\}$ e $\{5, 7, 9\}$ não são disjuntos. Por outro lado, (iii) é uma partição de S.

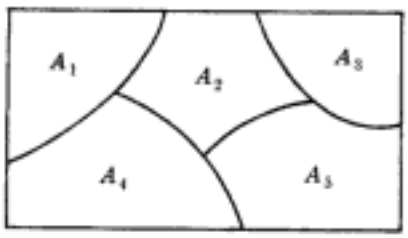


Fig. 1-11

Generalização de Operações entre Conjuntos

As operações de união e interseção entre dois conjuntos foram definidas acima. Tais operações podem ser estendidas para um número finito ou infinito de conjuntos como segue.

Considere primeiramente um número finito de conjuntos, $A_1, A_2, \ldots, A_m$. A união e a interseção desses conjuntos é, repectivamente, denotada e definida por:

$$A_1 \cup A_2 \cup \cdots \cup A_m = \cup_{i=1}^{m} A_i = \{x: x \in A_i \text{ para algum } A_i\} \text{ e}$$
$$A_1 \cap A_2 \cap \cdots \cap A_m = \cap_{i=1}^{m} A_i = \{x: x \in A_i \text{ para todo } A_i\}$$

Isto é, a união consiste nos elementos que pertencem a pelo menos um dos conjuntos, e a interseção consiste nos elementos que pertencem a todos os conjuntos.

Seja $\mathbf{A}$ uma coleção qualquer de conjuntos. A união e a interseção de conjuntos na coleção $\mathbf{A}$ são denotadas e definidas, respectivamente, por

$$\cup(A: A \in \mathbf{A}) = \{x: x \in A \text{ para algum } A \in \mathbf{A}\} \text{ e}$$
$$\cap(A: A \in \mathbf{A}) = \{x: x \in A \text{ para todo } A \in \mathbf{A}\}.$$

Isto é, a união consiste nos elementos que pertencem a pelo menos um dos conjuntos da coleção $\mathbf{A}$, e a interseção consiste nos elementos que pertencem a todos os conjuntos da coleção $\mathbf{A}$.

Exemplo 1.11 Considere os conjuntos

$$A_1 = \{1, 2, 3, \ldots\} = \mathbf{N}, \qquad A_2 = \{2, 3, 4, \ldots\}, \qquad A_3 = \{3, 4, 5, \ldots\}, \qquad A_n = \{n, n+1, n+2, \ldots\}.$$

A união e a interseção dos conjuntos são:

$$\cup(A_n: n \in \mathbf{N}) = \mathbf{N} \quad \text{e} \quad \cap(A_n: n \in \mathbf{N}) = \varnothing.$$

As Leis de DeMorgan também são válidas para as operações generalizadas definidas acima. Isto é:

Teorema 1-7: seja $\mathbf{A}$ uma coleção de conjuntos. Então:

(i) $(\cup(A: A \in \mathbf{A}))^c = \cap(A^c: A \in \mathbf{A})$,
(ii) $(\cap(A: A \in \mathbf{A}))^c = \cup(A^c: A \in \mathbf{A})$.

1.10 INDUÇÃO MATEMÁTICA

Uma propriedade essencial do conjunto

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

que é usada em muitas demonstrações é a seguinte:

Princípio de indução matemática I: Seja P uma proposição definida nos inteiros positivos $\mathbf{N}$, i.e., $P(n)$ é verdadeiro ou falso para cada n em $\mathbf{N}$. Suponha que P tem as seguintes propriedades:

(i) $P(1)$ é verdade.
(ii) $P(n + 1)$ é verdade sempre que $P(n)$ é verdade.

Então, P é verdade para todo inteiro positivo.

Vamos demonstrar esse princípio. Na verdade, quando **N** é descrito axiomaticamente, esse princípio é usualmente um dos axiomas.

Exemplo 1.12 Seja P a proposição de que a soma dos n primeiros números ímpares é n^2; isto é,

$$P(n)\colon\ 1 + 3 + 5 + \ldots + (2n - 1) = n^2.$$

(O n-ésimo número é $2n - 1$, e o número ímpar seguinte é $2n + 1$). Observe que $P(n)$ é verdade para $n = 1$, isto é,

$$P(1)\colon\ 1 = 1^2$$

Supondo que $P(n)$ é verdade, adicionamos $2n + 1$ a ambos os lados de $P(n)$ para obter

$$1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2,$$

que é $P(n + 1)$. Isto é, $P(n + 1)$ é verdade se $P(n)$ é verdade. Pelo princípio da indução matemática, P é verdade para todo n.

Existe uma forma do princípio de indução matemática que por vezes é mais conveniente de ser usada. Embora pareça diferente, na verdade, é equivalente ao princípio de indução.

Princípio de indução matemática II: Seja P uma proposição definida nos inteiros positivos **N** tal que:

(i) $P(1)$ é verdade.
(ii) $P(n)$ é verdade se $P(k)$ é verdade para todo $1 \leq k < n$.

Então, P é verdade para todo inteiro positivo.

Observação: Algumas vezes, se quer provar que a proposição P é verdade para o conjunto de inteiros

$$\{a,\ a + 1,\ a + 2, \ldots\},$$

onde a é algum inteiro, possivelmente zero. Isso pode ser feito substituindo 1 por a em qualquer um dos princípios de indução matemática acima.

Problemas Resolvidos

Conjuntos e subconjuntos

1.1 Quais dentre estes conjuntos são iguais: $\{r, t, s\}$, $\{s, t, r, s\}$, $\{t, s, t, r\}$, $\{s, r, s, t\}$?

Todos são iguais. Reordenação e repetição não alteram o conjunto.

1.2 Liste os elementos dos seguintes conjuntos; aqui, $\mathbf{N} = \{1, 2, 3, \ldots\}$.

(*a*) $A = \{x\colon x \in \mathbf{N},\ 3 < x < 12\}$
(*b*) $B = \{x\colon x \in \mathbf{N},\ x \text{ é par},\ x < 15\}$
(*c*) $C = \{x\colon x \in \mathbf{N},\ 4 + x = 3\}$

(*a*) A é composto dos inteiros positivos entre 3 e 12; portanto,

$$A = \{4, 5, 6, 7, 8, 9, 10, 11\}.$$

(*b*) B é composto dos inteiros pares menores do que 15; portanto,

$$B = \{2, 4, 6, 8, 10, 12, 14\}.$$

(*c*) Não existem inteiros positivos satisfazendo a condição $4 + x = 3$; portanto, C não contém nenhum elemento. Em outras palavras, $C = \varnothing$, o conjunto vazio.

1.3 Considere os seguintes conjuntos:

$$\varnothing, \quad A = \{1\}, \quad B = \{1, 3\}, \quad C = \{1, 5, 9\}, \quad D = \{1, 2, 3, 4, 5\},$$
$$E = \{1,3,5,7,9\}, \quad U = \{1,2,\ldots,8,9\}.$$

Insira o símbolo correto, $\subseteq$ ou $\not\subseteq$, em cada par de conjuntos:

(a) $\varnothing$, A (c) B, C (e) C, D (g) D, E
(b) A, B (d) B, E (f) C, E (h) D, U

(a) $\varnothing \subseteq A$ porque $\varnothing$ é um subconjunto de todo conjunto.

(b) $A \subseteq B$ porque 1 é o único elemento de A e pertence a B.

(c) $B \not\subseteq C$ porque $3 \in B$ mas $3 \notin C$.

(d) $B \subseteq E$ porque os elementos de B também pertencem a E.

(e) $C \not\subseteq D$ porque $9 \in C$ mas $9 \notin D$.

(f) $C \subseteq E$ porque os elementos de C também pertencem a E.

(g) $D \not\subseteq E$ porque $2 \in D$, mas $2 \notin E$.

(h) $D \subseteq U$ porque os elementos de D também pertencem a U.

1.4 Mostre que $A = \{2, 3, 4, 5\}$ não é um subconjunto de $B = \{x : x \in \mathbf{N}, x \text{ é par}\}$.

É necessário mostrar que pelo menos um elemento em A não pertence a B. Assim, $3 \in A$ e, como B consiste nos inteiros pares, $3 \notin B$; logo, A não é um subconjunto de B.

1.5 Mostre que $A = \{2, 3, 4, 5\}$ é um subconjunto próprio de $C = \{1, 2, 3, \ldots, 8, 9\}$.

Todo elemento de A pertence a C e, portanto, $A \subseteq C$. Por outro lado, $1 \in C$ mas $1 \notin A$, logo $A \neq C$. Portanto, A é um subconjunto próprio de C.

Operações entre Conjuntos

Os Problemas 1.6 e 1.8 se referem ao conjunto universo $U = \{1, 2, \ldots, 9\}$ e aos conjuntos

$$A = \{1, 2, 3, 4, 5\}, \quad C = \{5, 6, 7, 8, 9\}, \quad E = \{2, 4, 6, 8\}$$
$$B = \{4, 5, 6, 7\}, \quad D = \{1, 3, 5, 7, 9\}, \quad F = \{1, 5, 9\}$$

1.6 Determine:

(a) $A \cup B$ e $A \cap B$ (c) $A \cup C$ e $A \cap C$ (e) $E \cup E$ e $E \cap E$
(b) $B \cup D$ e $B \cap D$ (d) $D \cup E$ e $D \cap E$ (f) $D \cup F$ e $D \cap F$

Lembre que a união $X \cup Y$ consiste nos elementos em X ou Y (ou ambos), e que a interseção $X \cap Y$ consiste nos elementos em ambos, X e Y.

(a) $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ $A \cap B = \{4, 5\}$
(b) $B \cup D = \{1, 3, 4, 5, 6, 7, 9\}$ $B \cap D = \{5, 7\}$
(c) $A \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = U$ $A \cap C = \{5\}$
(d) $D \cap E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} = U$ $D \cap E = \varnothing$
(e) $E \cup E = \{2, 4, 6, 8\} = E$ $E \cap E = \{2, 4, 6, 8\} = E$
(f) $D \cup F = \{1, 3, 5, 7, 9\} = D$ $D \cap F = \{1, 5, 9\} = F$

Observe que $F \subseteq D$; portanto, pelo Teorema 1.2, devemos ter $D \cup F = D$ e $D \cap F = F$.

1.7 Determine (a) A^c, B^c, D^c, E^c; (b) $A \backslash B$, $B \backslash A$, $D \backslash E$, $F \backslash D$; (c) $A \oplus B$, $C \oplus D$, $E \oplus F$.

Lembre que:

(1) O complementar X^c consiste nos elementos no conjunto universo U que não pertencem a X.

(2) A diferença $X \backslash Y$ consiste dos elementos de X que não estão em Y.

(3) A diferença simétrica $X \oplus Y$ consiste nos elementos de X ou Y mas não de ambos X e Y.

Portanto:

(*a*) $A^c = \{6,7,8,9\}$; $B^c = \{1,2,3,8,9\}$; $D^c = \{2,4,6,8\} = E$; $E^c = \{1,3,5,7,9\} = D$.

(*b*) $A\backslash B = \{1,2,3\}$; $B\backslash A = \{6,7\}$; $D\backslash E = \{1,3,5,7,9\} = D$; $F\backslash D = \varnothing$.

(*c*) $A \oplus B = \{1,2,3,6,7\}$; $C \oplus D = \{1,3,8,9\}$; $E \oplus F = \{2,4,6,8,1,5,9\} = E \cup F$.

1.8 Determine (*a*) $A \cap (B \cup E)$; (*b*) $(A\backslash E)^c$; (*c*) $(A \cap D)\backslash B$; (*d*) $(B \cap F) \cup (C \cap E)$.

(*a*) Primeiramente compute $B \cup E = \{2,4,5,6,7,8\}$. Então, $A \cap (B \cup E) = \{2,4,5\}$.

(*b*) $A\backslash E = \{1,3,5\}$. Então, $(A\backslash E)^c = \{2,4,6,7,8,9\}$.

(*c*) $A \cap D = \{1,3,5\}$. Conclua $(A \cap D)\backslash B = \{1,3\}$.

(*d*) $B \cap F = \{5\}$ e $C \cap E = \{6,8\}$. Portanto, $(B \cap F) \cup (C \cap E) = \{5,6,8\}$.

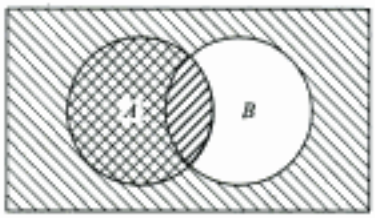
1.9 Mostre que é possível que $A \cap B = A \cap C$ sem que $B = C$.

Sejam $A = \{1,2\}$, $B = \{2,3\}$ e $C = \{2,4\}$. Então $A \cap B = \{2\}$ e $A \cap C = \{2\}$. Logo, $A \cap B = A \cap C$.

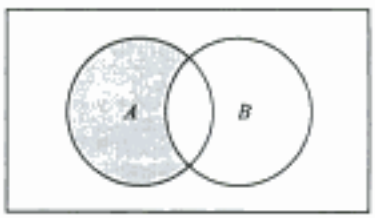
Diagramas de Venn

1.10 Considere o diagrama de Venn de dois conjuntos arbitrários A e B na Figura 1-1(*c*). Assinale os conjuntos: (*a*) $A \cap B^c$; (*b*) $(B\backslash A)^c$.

(*a*) Primeiramente marque a área que representa A tracejando em uma direção (////) e depois marque a área que representa B^C (a área fora de B) tracejando em outra direção (\\\\), como mostra a Figura1-12(*a*). A área com tracejado nas duas direções é a interseção desses dois conjuntos e representa $A \cap B^c$. De fato, $A\backslash B$ é às vezes definido como $A \cap B^c$.



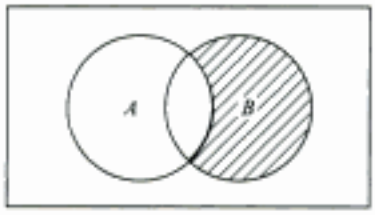
(*a*) A e B^c estão tracejados



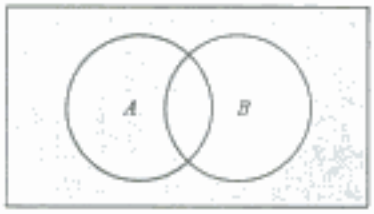
(*b*) $A \cap B^c$ está sombreado

Fig. 1-12

(*b*) Primeiramente marque a área que representa $B\backslash A$ (a área de B que não está em A) como na Figura 1-13(*a*). A área fora da região marcada, mostrada na Figura 1-13(*b*), representa $(B\backslash A)^C$.



(*a*) $B\backslash A$ está assinalada



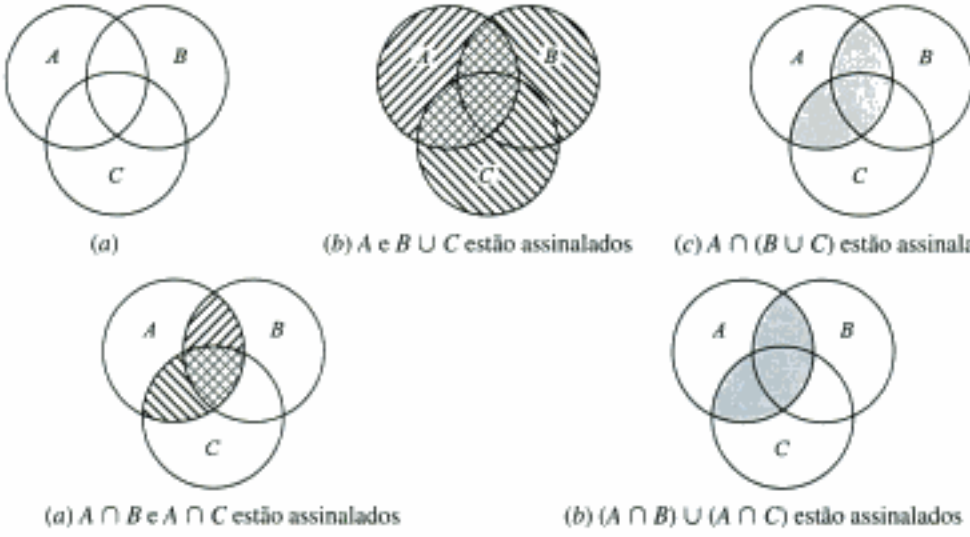
(*b*) $(B\backslash A)^C$ está assinalada

Fig. 1-13

1.11 Ilustre a lei de distributividade $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ com diagramas de Venn.

Desenhe três círculos se intersecionando assinalados com A, B e C, como na Figura 1-14(*a*). Agora, como na Figura 1-14(*b*), preencha A com traços em uma direção e $B \cup C$ com traços em outra direção; a área tracejada nas duas direções é $A \cap (B \cap C)$ como na Figura 1-14(*c*). Preencha então $A \cap B$ e $(A \cap C)$ como na Figura 1-14(*d*); a área total marcada é $(A \cap B) \cup (A \cap C)$, como na Figura 1-14(*e*).

Como esperado pela lei de distributividade, $A \cap (B \cup C)$ e $(A \cap B) \cup (A \cap C)$ são representados pelos mesmos pontos.



(*a*) (*b*) A e $B \cup C$ estão assinalados (*c*) $A \cap (B \cup C)$ estão assinalados

(*a*) $A \cap B$ e $A \cap C$ estão assinalados (*b*) $(A \cap B) \cup (A \cap C)$ estão assinalados

Fig. 1-14

1.12 Determine a validade do seguinte argumento:

S_1 : Todos meus amigos são músicos.
S_2 : João é meu amigo.
S_3 : Nenhum dos meus vizinhos é músico.

S : João não é meu vizinho.

As premissas S_1 e S_3 permitem construir o diagrama de Venn como na Figura 1-15. Por S_2, João pertence ao conjunto de amigos que é disjunto do conjunto de vizinhos. Logo, S é uma conclusão válida e, portanto, o argumento é válido.

Fig. 1-15

Conjuntos Finitos e Princípio da Enumeração

1.13 Determine quais dos seguintes conjuntos são finitos:

(*a*) $A = \{\text{estações do ano}\}$ (*b*) $B = \{\text{estados nos Estados Unidos}\}$
(*c*) $C = \{\text{inteiros positivos menores do que 1}\}$ (*d*) $D = \{\text{inteiros ímpares}\}$
(*e*) $E = \{\text{divisores inteiros positivos de 12}\}$ (*f*) $F = \{\text{gatos que vivem nos Estados Unidos}\}$

(*a*) A é finito pois existem quatro estações no ano, i.e., $n(A) = 4$.

(*b*) B é finito porque existem 50 estados nos Estados Unidos, i.e., $n(B) = 50$.

(*c*) Não existem inteiros positivos menores do que 1; logo, C é vazio. Portanto, C é finito e $n(C) = 0$.

(*d*) D é infinito.

(*e*) Os divisores inteiros positivos de 12 são 1, 2, 3, 4, 6 e 12. Portanto, E é finito e $n(E) = 6$.

(*f*) Embora possa ser difícil determinar o número de gatos que vivem nos Estados Unidos, existe um número finito deles em qualquer tempo. Portanto, F é finito.

1.14 Em uma pesquisa com 60 pessoas, verificou-se que:

25 lêem a *Newsweek*,
26 lêem *Time*,
26 lêem *Fortune*,
9 lêem *Newsweek* e *Fortune*,
11 lêem *Newsweek* e *Time*,

8 lêem *Time* e *Fortune*,
3 lêem as três revistas.

(*a*) Ache o número de pessoas que lêem pelo menos uma das três revistas.
(*b*) Preencha, com o número correto de pessoas, cada uma das oito regiões no diagrama de Venn na Figura 1-16(*a*), onde N, T e F denotam, respectivamente, o conjunto de pessoas que lêem *Newsweek*, *Time* e *Fortune*.
(*c*) Ache o número de pessoas que lêem exatamente uma revista.

(*a*) Queremos $n(N \cup T \cup F)$. Pelo Corolário 1.6,

$$n(N \cup T \cup F) = n(N) + n(T) + n(F) - n(N \cap T) - n(N \cap F) - n(T \cap F) + n(N \cap T \cap F)$$

$$= 25 + 26 + 26 - 11 - 9 - 8 + 3 = 52.$$

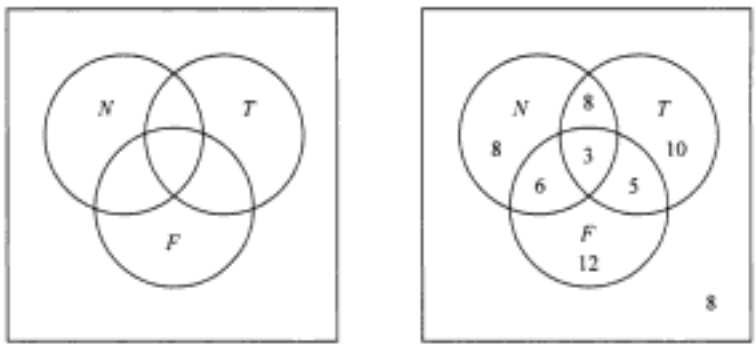


Fig. 1-16

(*b*) O diagrama de Venn, obtido na Figura 1-16(*b*), mostra o seguinte:

3 lêem as três revistas;
$11 - 3 = 8$ lêem *Newsweek* e *Time*, mas não as três revistas;
$9 - 3 = 6$ lêem *Newsweek* e *Fortune*, mas não as três revistas;
$8 - 3 = 5$ lêem *Time* e *Fortune*, mas não as três revistas;
$25 - 8 - 6 - 3 = 8$ lêem apenas a *Newsweek*;
$26 - 8 - 5 - 3 = 10$ lêem apenas *Time*;
$26 - 6 - 5 - 3 = 12$ lêem apenas *Fortune*;
$60 - 52 = 8$ não lêem revista alguma.

(*c*) $8 + 10 + 12 = 30$ lêem apenas uma revista.

Álgebra de Conjuntos e Dualidade

1.15 Escreva a equação dual de cada uma das equações a seguir.

(*a*) $(U \cap A) \cup (B \cap A) = A$
(*b*) $(A \cup B \cup C)^c = (A \cup C)^c \cap (A \cup B)^c$
(*c*) $(A \cap U) \cap (\varnothing \cup A^c) = \varnothing$
(*d*) $(A \cap U)^c \cap A = \varnothing$

Trocando $\cup$ por $\cap$ e também U por $\varnothing$ em cada equação:

(*a*) $(\varnothing \cup A) \cap (B \cup A) = A$
(*b*) $(A \cap B \cap C)^c = (A \cap C)^c \cup (A \cap B)^c$
(*c*) $(A \cup \varnothing) \cup (U \cap A^c) = U$
(*d*) $(A \cup \varnothing)^c \cup A = U$

1.16 Prove as leis de comutatividade: (*a*) $A \cup B = B \cup A$ e (*b*) $A \cap B = B \cap A$.

(*a*) $A \cup B = \{x: x \in A \text{ ou } x \in B\} = \{x: x \in B \text{ ou } x \in A\} = B \cup A$.
(*b*) $A \cap B = \{x: x \in A \text{ e } x \in B\} = \{x: x \in B \text{ e } x \in A\} = B \cap A$.

1.17 Prove a seguinte identidade: $(A \cup B) \cap (A \cup B^c) = A$.

	Afirmativa	Justificativa
1.	$(A \cup B) \cap (A \cup B^c) = A \cup (B \cap B^c)$	Lei de Distributividade
2.	$B \cap B^c = \varnothing$	Lei dos complementares
3.	$(A \cup B) \cap (A \cup B^c) = A \cup \varnothing$	Substituição
4.	$A \cup \varnothing = A$	Lei da Identidade
5.	$(A \cup B) \cap (A \cup B^c) = A$	Substituição

1.18 Prove: $(A \cup B) \backslash (A \cap B) = (A \backslash B) \cup (B \backslash A)$. (Logo, qualquer uma das sentenças pode ser usada para definir $A \oplus B$.)

Usando $X \backslash Y = X \cap Y^c$ e as leis da Tabela 1-1, incluindo as leis de DeMorgan, obtemos:

$$\begin{aligned}(A \cup B) \backslash (A \cap B) &= (A \cup B) \cap (A \cap B)^c = (A \cup B) \cap (A^c \cup B^c) \\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) \\ &= \varnothing \cup (A \cap B^c) \cup (B \cap A^c) \cup \varnothing \\ &= (A \cap B^c) \cup (B \cap A^c) = (A \backslash B) \cup (B \backslash A).\end{aligned}$$

Classes de Conjuntos

1.19 Ache os elementos do conjunto $A = [\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8\}]$.

A é uma classe de conjuntos; seus elementos são os conjuntos $\{1, 2, 3\}$, $\{4, 5\}$ e $\{6, 7, 8\}$.

1.20 Considere a classe A de conjuntos do Problema 1.19. Determine se cada uma das afirmativas seguintes é verdadeira ou falsa:

(*a*) $1 \in A$ (*c*) $\{6, 7, 8\} \in A$ (*e*) $\varnothing \in A$

(*b*) $\{1, 2, 3\} \subseteq A$ (*d*) $\{\{4, 5\}\} \subseteq A$ (*f*) $\varnothing \subseteq A$

(*a*) Falso. 1 não é um elemento de A.

(*b*) Falso. {1,2,3} não é um subconjunto de A; é um elemento de A.

(*c*) Verdadeiro. {6,7,8} é um elemento de A.

(*d*) Verdadeiro. [{4,5}], o conjunto composto do elemento {4,5}, é um elemento de A.

(*e*) Falso. O conjunto vazio não é um elemento de A, i. e., não é um dos três elementos listados como elementos de A.

(*f*) Verdadeiro. O conjunto vazio é um subconjunto de todo conjunto, inclusive de uma classe de conjuntos.

1.21 Determine o conjunto das partes de A Partes(A) de $A = \{a,b,c,d\}$.

Os elementos de Partes(A) são os subconjuntos de A. Portanto,

$$\begin{aligned}\text{Partes}(A) = [&A, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b\}, \{a, c\}, \\ &\{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a\}, \{b\}, \{c\}, \{d\}, \varnothing]\end{aligned}$$

Como se poderia esperar, Partes(A) possui $2^4 = 16$ elementos.

1.22 Seja $S = 5\{vermelho, azul, verde, amarelo\}$. Determine quais das seguintes classes são partições de S:

(*a*) $P_1 = [\{vermelho\}, \{azul, verde\}]$. (*c*) $P_3 = [\varnothing, \{vermelho, azul\}, \{verde, amarelo\}]$.

(*b*) $P_2 = [\{vermelho, azul, verde, amarelo\}]$. (*d*) $P_4 = [\{azul\}, \{vermelho, amarelo, verde\}]$.

(*a*) Não, pois *amarelo* não pertence a nenhuma célula.

(*b*) Sim, pois P_2 é uma partição de S, cujo único elemento é o próprio S.

(*c*) Não, pois o conjunto vazio $\varnothing$ não pode pertencer a nenhuma partição.

(*d*) Sim, pois cada elemento de S aparece exatamente em uma célula.

1.23 Ache todas as partições de $S = \{1, 2, 3\}$.

Observe que cada partição de S contém 1, 2 ou 3 células. As partições que contêm cada uma destas quantidades de células são:

(1): $[S]$

(2): $[\{1\}, \{2, 3\}]$, $[\{2\}, \{1, 3\}]$, $[\{3\}, \{1, 2\}]$

(3): $[\{1\}, \{2\}, \{3\}]$

Portanto, vemos que existem cinco partições diferentes de S.

Problemas Diversos

1.24 Prove a proposição P de que a soma dos primeiros n inteiros positivos é igual a $\frac{1}{2}n(n+1)$; isto é,

$$P(n): \qquad 1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1).$$

A proposição vale para $n=1$, pois

$$P(1): 1 = \tfrac{1}{2}(1)(1+1).$$

Supondo que $P(n)$ é verdade, somamos $n+1$ a ambos os lados de $P(n)$, obtendo:

$$\begin{aligned} 1 + 2 + 3 + \cdots + n + (n+1) &= \tfrac{1}{2}n(n+1) + (n+1) \\ &= \tfrac{1}{2}[n(n+1) + 2(n+1)] \\ &= \tfrac{1}{2}[(n+1)(n+2)], \end{aligned}$$

que é $P(n+1)$. Isto é, $P(n+1)$ é verdade se $P(n)$ é verdade. Pelo princípio de indução, P é verdade para todo n.

1.25 Prove a seguinte proposição para $(n \geq 0)$:

$$P(n): \quad 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$$

$P(0)$ é verdade, pois $1 = 2^1 - 1$. Supondo que $P(n)$ é verdade, somamos 2^{n+1} a ambos os lados de $P(n)$, obtendo

$$\begin{aligned} 1 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} &= 2^{n+1} - 1 + 2^{n+1} \\ &= 2(2^{n+1}) - 1 \\ &= 2^{n+2} - 1, \end{aligned}$$

que é $P(n+1)$. Portanto, $P(n+1)$ é verdade se $P(n)$ é verdade. Pelo princípio de indução, P é verdade para todo $n \geq 0$.

1.26 Prove: $(A \cap B) \subseteq A \subseteq (A \cup B)$ e $(A \cap B) \subseteq B \subseteq (A \cup B)$.

Já que todo elemento de $A \cap B$ está em ambos A e B, é certamente verdade que, se $x \in (A \cap B)$, então $x \in A$. Portanto, $(A \cap B) \subseteq A$. Além disso, se $x \in A$, então $x \in (A \cap B)$ (pela definição de $A \cup B$), logo $A \subseteq (A \cup B)$. Juntando-se tudo, obtêm-se, $(A \cap B) \subseteq A \subseteq (A \cup B)$. De maneira similar, $(A \cap B) \subseteq B \subseteq (A \cup B)$.

1.27 Prove o Teorema 1.2: são equivalentes $A \subseteq B$, $A \cap B = A$ e $A \cup B = B$.

Suponha que $A \subseteq B$ e seja $x \in A$. Então $x \in B$, já que $x \in A \cap B$ e $A \subseteq A \cap B$. Pelo Problema 1.26, $(A \cap B) \subseteq A$. Portanto, $A \cap B = A$. Por outro lado, suponha que $A \cap B = A$, e seja $x \in A$. Então $x \in (A \cap B)$, pois $x \in A$ e $x \in B$. Portanto, $A \subseteq B$. Ambos os resultados mostram que $A \subseteq B$ é equivalente a $A \cap B = A$.

Suponha novamente que $A \subseteq B$. Seja $x \in (A \cap B)$. Então, $x \in A$ ou $x \in B$. Se $x \in A$, então $x \in B$ porque $A \subseteq B$. Em qualquer caso, $x \in B$. Portanto, $A \cup B \subseteq B$. Pelo Problema 1.26, $B \subseteq A \cup B$. Portanto, $A \cup B = B$. Agora suponha que $A \cup B = B$, e seja $x \in A$. Então $x \in A \cup B$ pela definição de união de conjuntos. Logo, $x \in B = A \cup B$. Portanto, $A \subseteq B$. Ambos os resultados mostram que $A \subseteq B$ é equivalente a $A \cup B = B$.

Logo, $A \subseteq B$, $A \cap B = A$ e $A \cup B = B$ são equivalentes.

1.28 Prove o Teorema 1.5: se A e B são conjuntos finitos, então $A \cup B$ e $A \cap B$ são finitos e

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Se A e B são finitos, então é claro que, $A \cap B$ e $A \cup B$ são finitos.

Suponha que contemos os elementos de A e depois contemos os elementos de B. Então, todo elemento em $A \cap B$ seria contado duas vezes: uma vez em A e outra em B. Portanto,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Uma alternativa de prova é considerar o Problema 1.36 e escrever: A é a união disjunta de $A\backslash B$ e $A \cap B$; B é a união disjunta de $B\backslash A$ e $A \cap B$; e $A \cup B$ é a união disjunta de $A\backslash B$, $A \cap B$ e $B\backslash A$. Portanto, pelo Lema 1.4,

$$\begin{aligned} n(A \cup B) &= n(A\backslash B) + n(A \cap B) + n(B\backslash A) \\ &= n(A\backslash B) + n(A \cap B) + n(B\backslash A) + n(A \cap B) - n(A \cap B) \\ &= n(A) + n(B) - n(A \cap B). \end{aligned}$$

Problemas Complementares

Conjuntos e Subconjuntos

1.29 Quais dos seguintes conjuntos são iguais?

$A = \{x: x^2 - 4x + 3 = 0\}$, $C = \{x: x \in \mathbf{N}, x < 3\}$, $E = \{1, 2\}$, $G = \{3, 1\}$,

$B = \{x: x^2 - 3x + 2 = 0\}$, $D = \{x: x \in \mathbf{N}, x \text{ é ímpar}, x < 5\}$ $F = \{1, 2, 1\}$, $H = \{1, 1, 3\}$.

1.30 Liste os elementos dos conjuntos seguintes considerando o conjunto universo $U = \{a, b, c, \ldots, y, z\}$. Identifique também os conjuntos iguais, se existirem.

$A = \{x : x \text{ é vogal}\}$ $C = \{x : x \text{ precede "f" no alfabeto}\}$

$B = \{x : x \text{ é uma letra na palavra } \textit{"little"}\}$ $D = \{x : x \text{ é uma letra na palavra } \textit{"title"}\}$

1.31 Seja $A = \{1, 2, \ldots, 8, 9\}$, $B = \{2, 4, 6, 8\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{3, 4, 5\}$, $E = \{3, 5\}$.

(*a*) X e B são disjuntos. (*c*) $X \subseteq A$ mas $X \nsubseteq C$.

(*b*) $X \subseteq D$ mas $X \nsubseteq B$. (*d*) $X \subseteq C$ mas $X \nsubseteq A$.

Operações entre Conjuntos

Os Problemas 1.32 a 1.34 se referem aos conjuntos $U = \{1, 2, 3, \ldots, 8, 9\}$ e $A = \{1, 2, 5, 6\}$, $B = \{2, 5, 7\}$, $C = \{1, 3, 5, 7, 9\}$.

1.32 Encontre: (*a*) $A \cap B$ e $A \cap C$; (*b*) $A \cup B$ e $B \cup C$; (*c*) A^c e C^c.

1.33 Encontre: (*a*) $A\backslash B$ e $A\backslash C$; (*b*) $A \oplus B$ e $A \oplus C$.

1.34 Encontre: (*a*) $(A \cup C)\backslash B$; (*b*) $(A \cup B)^c$; (*c*) $(B \oplus C)\backslash A$.

1.35 Sejam: $A = \{a, b, c, d, e\}$, $B = \{a, b, d, f, g\}$, $C = \{b, c, e, g, h\}$, $D = \{d, e, f, g, h\}$.
Ache:

(*a*) $A \cup B$ (*d*) $A \cap (B \cup D)$ (*g*) $(A \cup D)\backslash C$ (*j*) $A \oplus B$

(*b*) $B \cap C$ (*e*) $B\backslash(C \cup D)$ (*h*) $B \cap C \cap D$ (*k*) $A \oplus C$

(*c*) $C\backslash D$ (*f*) $(A \cap D) \cup B$ (*i*) $(C\backslash A)\backslash D$ (*l*) $(A \oplus D)\backslash B$

1.36 Sejam A e B conjuntos quaisquer. Mostre:

(*a*) A é a união disjunta de $A\backslash B$ e $A \cap B$.

(*b*) $A \cup B$ é a união disjunta de $A\backslash B$, $A \cap B$ e $B\backslash A$.

1.37 Prove:

(*a*) $A \subseteq B$ se e somente se $A \cap B^c = \varnothing$.

(*b*) $A \subseteq B$ se e somente se $A^c \cup B = U$.

(*c*) $A \subseteq B$ se e somente se $B^c \subseteq A^c$.

(*d*) $A \subseteq B$ se e somente se $A\backslash B = \varnothing$.

(Compare os resultados com o Teorema 1.2.)

1.38 Prove as leis de absorção: (*a*) $A \cup (A \cap B) = A$; (*b*) $A \cap (A \cup B) = A$.

1.39 A fórmula $A \backslash B = A \cap B^c$ define a operação de diferença em termos da operação de interseção e de complementar. Ache uma fórmula que defina a união $A \cup B$ em termos da operação de interseção e de complementar.

Diagramas de Venn

1.40 O diagrama de Venn na Figura 1-17 apresenta os conjuntos A, B e C. Assinale os seguintes conjuntos: (*a*) $A \backslash (B \cup C)$; (*b*) $A^c \cap (B \cup C)$; (*c*) $A^c \cap (C \backslash B)$.

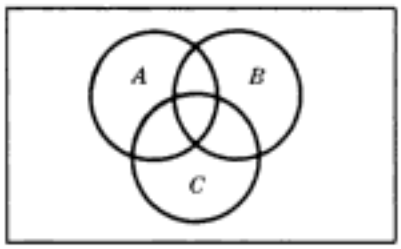


Fig. 1-17

1.41 Use o diagrama Venn da Fig. 1-6 e o Exemplo 1.6 para escrever cada um dos conjuntos como a união disjunta dos produtos fundamentais:

(*a*) $A \cap (B \cup C)$, (*b*) $A^c \cap (B \cup C)$, (*c*) $A \cup (B \backslash C)$.

1.42 Esboce um diagrama de Venn para os conjuntos A, B e C, onde $A \subseteq B$, os conjuntos B e C são disjuntos, mas A e C têm elementos em comum.

Álgebra de Conjuntos e Dualidade

1.43 Escreva a equação dual de cada uma das equações:

(*a*) $A \cup B = (B^c \cap A^c)^c$ (*b*) $A = (B^c \cap A) \cup (A \cap B)$

(*c*) $A \cup (A \cap B) = A$ (*d*) $(A \cap B) \cup (A^c \cap B) \cup (A \cap B^c) \cup (A^c \cap B^c) = U$

1.44 Use as leis da Tabela 1-1 para provar cada uma das identidades:

(*a*) $(A \cap B) \cup (A \cap B^c) = A$, (*b*) $A \cup (A \cap B) = A$,

(*c*) $A \cup B = (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B)$.

Conjuntos Finitos e o Princípio de Enumeração

1.45 Determine quais dos seguintes conjuntos são finitos.

(*a*) O conjunto das retas paralelas ao eixo x.

(*b*) O conjunto das letras do alfabeto.

(*c*) O conjunto dos números múltiplos de 5.

(*d*) O conjunto de animais que vivem na Terra.

(*e*) O conjunto de números que são soluções da equação $x^{27} + 26x^{18} - 17x^{11} + 7x^3 - 10 = 0$.

(*f*) O conjunto dos círculos contendo a origem (0, 0).

1.46 Use o Teorema 1.5 para provar o Corolário 1.6: se A, B e C são conjuntos finitos, então $A \cup B \cup C$ também é finito e

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C).$$

1.47 Foi realizada uma pesquisa com uma amostragem de 25 carros novos à venda em uma revendedora local para verificar quais dos três opcionais populares, ar-condicionado (A), rádio (R) e vidros elétricos (V), já estavam instalados. A pesquisa concluiu:

15 tinham ar-condicionado,

12 tinham rádio,

11 tinham vidros elétricos,
5 tinham ar-condicionado e vidros elétricos,
9 tinham ar-condicionado e rádio,
4 tinham rádio e vidros elétricos,
3 tinham as três opções.

Ache o número de carros que têm: (*a*) apenas vidros elétricos; (*b*) apenas ar-condicionado;(*c*) apenas rádio; (*d*) rádio e vidros elétricos, mas não ar-condicionado; (*e*) ar-condicionado e rádio, mas não vidros elétricos; (*f*) apenas uma das opções; (*h*) nenhuma das opções.

Classes de Conjuntos

1.48 Ache o conjunto das partes de A, Partes$(A) = \{1,2,3,4,5\}$.

1.49 Dado $A = [[a,b\}, \{c\}, \{d,e,f\}]$.

(*a*) Determine se cada uma das afirmativas seguintes é verdadeira ou falsa:

(i) $a \in A$, (ii) $\{c\} \subseteq A$, (iii) $\{d,e,f\} \in A$, (iv) $\{\{a,b\}\} \subseteq A$, (v) $\varnothing \subseteq A$.

(*b*) Ache o conjunto das partes de A.

1.50 Suponha que A seja um conjunto finito e $n(A) = m$. Mostre que Partes(A) tem 2^m elementos.

Partições

1.51 Seja $X = \{1, 2, \ldots, 8, 9\}$. Determine se cada uma das seguintes classes é ou não uma partição de X.

(*a*) $[\{1,3,6\}, \{2,8\}, \{5,7,9\}]$ (*c*) $[\{2,4,5,8\}, \{1,9\}, \{3,6,7\}]$
(*b*) $[\{1,5,7\}, \{2,4,8,9\}, \{3,5,6\}]$ (*d*) $[\{1,2,7\}, \{3,5\}, \{4,6,8,9\}, \{3,5\}]$

1.52 Seja $S = \{1, 2, 3, 4, 5, 6\}$. Determine se cada uma das seguintes classes é ou não uma partição de S.

(*a*) $P_1 = [\{1,2,3\}, \{1,4,5,6\}]$ (*c*) $P_3 = [\{1,3,5\}, \{2,4\}, \{6\}]$
(*b*) $P_2 = [\{1,2\}, \{3,5,6\}]$ (*d*) $P_4 = [\{1,3,5\}, \{2,4,6,7\}]$

1.53 Determine se cada uma das seguintes classes é ou não uma partição do conjunto de inteiros positivos N.

(*a*) $[\{n: n > 5\}, \{n: n < 5\}]$ (*b*) $[\{n: n > 5\}, \{0\}, \{1,2,3,4,5\}]$, (*c*) $[\{n: n^2 > 11\}, \{n: n^2 < 11\}]$

1.54 Sejam $\{A_1, A, \ldots, A_m\}$ e $\{B_1, B_2, \ldots, B_n\}$ partições de um conjunto X. Mostre que a coleção de conjuntos:

$$P = [A_i \cap B_j : i = 1, \ldots, m,\ j = 1, \ldots, n] \backslash \varnothing$$

também é uma partição (chamada de *cross partition*[†]) de X (observe que o conjunto vazio, $\varnothing$, foi retirado).

1.55 Seja $X = \{1, 2, 3, \ldots, 8, 9\}$. Ache a *cross partition* P das seguintes partições de X:

$$P_1 = [\{1,3,5,7,9\},\ \{2,4,6,8\}] \quad \text{e} \quad P_2 = [\{1,2,3,4\},\ \{5,7\},\ \{6,8,9\}.$$

Argumentos e Diagramas de Venn

1.56 Use um diagrama de Venn para mostrar que o seguinte argumento é válido:

S_1: Bebês são ilógicos.
S_2: Ninguém que possa lidar com crocodilos é desprezado.
S_3: Pessoas ilógicas são desprezadas.

S: Bebês não podem lidar com crocodilos.

(Esse argumento foi retirado do livro *Symbolic logic*, de Lewis Carroll, o mesmo autor de *Alice no País das Maravilhas*.)

[†] N. de T. Optamos por deixar a expressão em inglês por não haver tradução consagrada.

1.57 Considere as seguintes hipóteses:

S_1: Todos os dicionários são úteis.
S_2: Maria possui apenas romances.
S_3: Nenhum romance é útil.

Determine a validade de cada uma das conclusões seguintes: (*a*) romances não são dicionários; (*b*) Maria não tem um dicionário; (*c*) todos livros úteis são dicionários.

Indução

1.58 Prove: $2 + 4 + 6 + \cdots + 2n = n(n + 1)$.

1.59 Prove: $1 + 4 + 7 + \cdots + (3n - 2) = 2n(3n - 1)$.

1.60 Prove: $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{1}{2n+1}$.

1.61 Prove: $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Problemas Variados

1.62 Suponha que $\mathbf{N} = \{1, 2, 3, \ldots\}$ seja o conjunto universo e $A = \{x: x \leq 6\}$, $B = \{x: 4 \leq x \leq 9\}$, $C = \{1, 3, 5, 7, 9\}$, $D = \{2, 3, 5, 7, 8\}$. Determine: (*a*) $A \oplus B$; (*b*) $B \oplus C$; (*c*) $A \cap (B \oplus D)$; (*d*) $(A \cap B) \oplus (A \cap D)$.

1.63 Prove as seguintes propriedades da diferença simétrica:

(i) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (lei da associatividade).
(ii) $A \oplus B = B \oplus A$ (lei de comutatividade).
(iii) Se $A \oplus B = A \oplus C$, então $B = C$ (lei do cancelamento).
(iv) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$ (lei de distributividade).

1.64 Considere n conjuntos distintos $A_1, A_2, \ldots, A_n$ em um conjunto universo U. Mostre:

(*a*) Existem 2^n produtos fundamentais dos n conjuntos.
(*b*) Quaisquer dois produtos fundamentais são disjuntos.
(*c*) U é a união de todos os produtos fundamentais.

Respostas dos Problemas Complementares

1.29 $B = C = E = F$; $A = D = G = H$.

1.30 $A = \{a, e, i, o, u\}$; $B = D = \{1, i, t, e\}$; $C = \{a, b, c, d, e\}$.

1.31 (*a*) C e E; (*b*) D e E; (*c*) A, B, D; (*d*) Nenhum.

1.32 (*a*) $A \cap B = \{2, 5\}$; $A \cap C = \{1, 5\}$. (*b*) $A \cup B = \{1, 2, 5, 6, 7\}$; $B \cup C = \{1, 2, 3, 5, 7, 9\}$.
(*c*) $A^c = \{3, 4, 7, 8, 9\}$; $C^c = \{2, 4, 6, 8\}$.

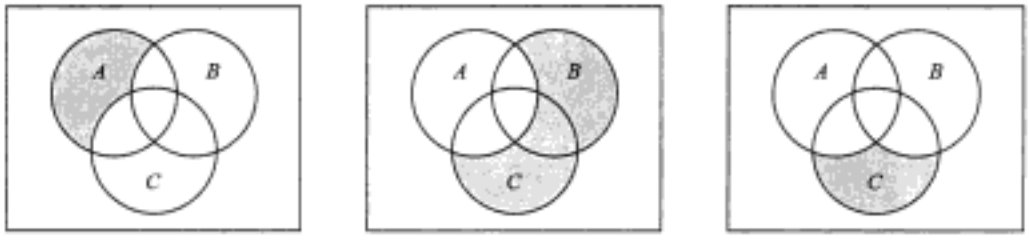
1.33 (*a*) $A \backslash B = \{1, 6\}$; $A \backslash C = \{2, 6\}$. (*b*) $A \oplus B = \{1, 6, 7\}$; $A \oplus C = \{2, 3, 6, 7, 9\}$.

1.34 (*a*) $(A \cup C) \backslash B = \{1, 3, 6, 9\}$. (*b*) $(A \cup B)^c = \{3, 4, 8, 9\}$. (*c*) $(B \oplus C) \backslash A = \{3, 9\}$.

1.35 (*a*) {a, b, c, d, e, f, g}; (*b*) {b, g}; (*c*) {b, c}; (*d*) {a, b, d, e}; (*e*) {a};
(*f*) {a, b, d, e, f, g}; (*g*) {a, d, f}; (*h*) {g}; (*i*) $\varnothing$; (*j*) {c, e, f, g}; (*k*) {a, d, y, h};
(*l*) {c, h}.

1.39 $A \cup B = (A^c \cap B^c)^c$

1.40 Veja Fig. 1-18.



(*a*) (*b*) (*c*)

Fig. 1-18

1.41 (*a*) $(A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C)$
(*b*) $(A^c \cap B \cap C^c) \cup (A^c \cap B \cap C) \cup (A^c \cap B^c \cap C)$
(*c*) $(A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C) \cup (A^c \cap B \cap C^c) \cup (A \cap B^c \cap C^c)$

1.42 Não existe um tal diagrama de Venn. Se A e C têm um elemento em comum x, e $A \subseteq B$, então x deve também pertencer a B. Logo, B e C também devem ter um elemento em comum.

1.43 (*a*) $A \cap B = (B^c \cup A^c)^c$; (*b*) $A = (B^c \cup A) \cap (A \cup B)$; (*c*) $A \cap (A \cup B) = A$;
(*d*) $(A \cup B) \cap (A^c \cup B) \cap (A \cup B^c) \cap (A^c \cup B^c) = \varnothing$.

1.45 (*a*) Infinito; (*b*) finito; (*c*) infinito; (*d*) finito; (*e*) finito; (*f*) infinito.

1.47 Use os dados preenchendo primeiramente o diagrama de Venn de A (ar-condicionado), R (rádio) e V (vidros elétricos) da Figura 1-19. Então: (*a*) 5; (*b*) 4; (*c*) 2; (*d*) 4; (*e*) 6; (*f*) 11; (*g*) 23; (*h*) 2.

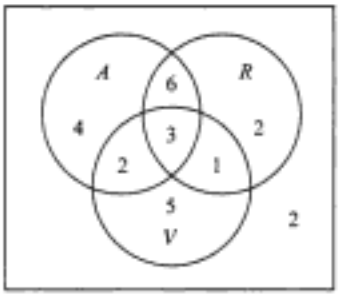


Fig. 1-19

1.48 Partes(A) tem $2^5 = 32$ elementos como descrito a seguir:

$[\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \{4,5\},$
$\{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{2,3,4\}, \{2,3,5\}, \{3,4,5\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,4,5\}, \{1,2,3,4\},$
$\{1,2,3,5\}, \{1,2,4,5\}, \{1,3,4,5\}, \{2,3,4,5\}, A]$.

1.49 (*a*) (i) Falsa; (ii) Falsa; (iii) Verdadeira; (iv) Verdadeira; (v) Falsa.
(*b*) Note que $n(A) = 3$; logo, Partes(A) tem $2^3 = 8$ elementos.

$$\text{Partes}(A) = \{A, [\{a,b\}, \{c\}], [\{a,b\}, \{d,e,f\}], [\{c\}, \{d,e,f\}], [\{a,b\}], [\{c\}], [\{d,e,f\}], \varnothing\}$$

1.50 Seja x um elemento arbitrário de Partes(A). Para cada $a \in A$, existem duas possibilidades: ou $a \in A$ ou $a \notin A$. Mas existem m elementos em A; portanto, existem $2 \cdot 2 \cdot \ldots \cdot 2 = 2^m$ diferentes conjuntos X. Isto é, Partes(A) tem 2^m elementos.

1.51 (*a*) Não, (*b*) não, (*c*) sim, (*d*) sim.

1.52 (*a*) Não, (*b*) não, (*c*) sim, (*d*) não.

1.53 (*a*) Não, (*b*) não, (*c*) sim.

1.55 $P = [\{1,3\}, \{5,7\}, \{9\}, \{2,4\}, \{8\}]$.

1.56 As três premissas conduzem ao diagrama de Venn da Figura 1-20. O conjunto de bebês e o conjunto de pessoas que podem lidar com crocodilos são disjuntos. Em outras palavras, a conclusão S é válida.

Fig. 1-20

1.57 As três premissas conduzem ao diagrama de Venn da Figura 1-21. Deste diagrama, segue que (*a*) e (*b*) são conclusões válidas. Entretanto, (*c*) não é uma conclusão válida, pois podem existir livros úteis que não sejam dicionários.

Fig. 1-21

1.62 (*a*) $\{1,2,3,7,8,9\}$; (*b*) $\{1,3,4,6,8\}$; (*c*) $\{2,3,4,6\}$; (*d*) $\{2,3,4,6\}$. [Note (*c*) = (*d*).]

Capítulo 2

Relações

2.1 INTRODUÇÃO

O leitor está familiarizado com muitas relações que são usadas em matemática e em ciência da computação, por exemplo, "menor do que", "é paralelo a", "é um subconjunto de", e assim por diante. Em um certo sentido, essas relações levam em consideração a existência ou não de determinadas conexões entre pares de objetos tomados em uma ordem definida. Formalmente, definimos uma relação em termos desses "pares ordenados".

Existem três tipos de relações que desempenham importantes papéis na nossa teoria: (i) relações de equivalência, (ii) relações de ordem e (iii) funções. As relações de equivalência estão fundamentalmente cobertas neste capítulo; as relações de ordem são apresentadas aqui, mas também serão discutidas no Capítulo 14; as funções são cobertas no próximo capítulo.

Como observado acima, as relações serão definidas em termos de pares ordenados (a, b) de elementos, onde a é designado como primeiro elemento e b como segundo elemento. Especificamente,

$$(a, b) = (c, d)$$

se e somente se $a = c$ e $b = d$. Portanto, $(a, b) \neq (b, a)$ a menos que $a = b$. Esse fato contrasta com a teoria de conjuntos estudada no Capítulo 1, em que a ordem dos elementos é irrelevante; por exemplo, $\{3, 5\} = \{5, 3\}$.

Apesar de as matrizes serem estudadas no Capítulo 5 incluímos aqui sua conexão com as relações para tratar do assunto de forma completa. Essas seções, entretanto, podem ser ignoradas em uma primeira leitura por aqueles que não possuem conhecimento prévio da teoria de matrizes.

2.2 PRODUTOS DE CONJUNTOS

Considere dois conjuntos arbitrários A e B. O conjunto de todos os pares ordenados (a, b) onde $a \in A$ e $b \in B$ é chamado de *produto* ou *produto cartesiano* de A e B. Uma designação abreviada desse produto é $A \times B$, que pode ser lida como "A cartesiano B ". Por definição,

$$A \times B = \{(a, b): a \in A \text{ e } b \in B\}.$$

Freqüentemente se escreve A^2 em vez de $A \times A$.

Exemplo 2.1 $\mathbf{R}$ denota o conjunto dos números reais, e $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ é o conjunto dos pares ordenados de números reais. O leitor está familiarizado com a representação geométrica de $\mathbf{R}^2$ por pontos no plano, como na Fig. 2-1. Aqui, cada ponto P representa um par ordenado (a, b) de números reais e vice-versa; a linha vertical contendo P intercepta o eixo x em a, e a linha horizontal contendo P intercepta o eixo y em b. $\mathbf{R}^2$ é freqüentemente chamado de *plano cartesiano*.

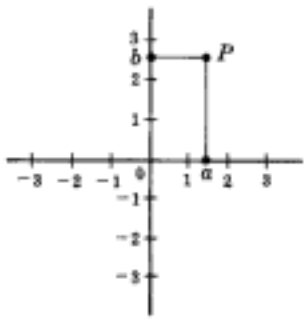


Fig. 2-1

Exemplo 2.2 Sejam $A = \{1,2\}$ e $B = \{a,b,c\}$. Então,

$$A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$$
$$B \times A = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$$

Também $A \times A = \{(1,1),(1,2),(2,1),(2,2)\}$

Existem dois fatos dignos de nota no exemplo acima. Primeiramente, $A \times B \neq B \times A$. O produto cartesiano diz respeito a pares ordenados de modo que, naturalmente, a ordem em que os conjuntos são considerados é importante. Em segundo lugar, usando $n(S)$ para o número de elementos em um conjunto S, temos

$$n(A \times B) = 6 = 2 \cdot 3 = n(A) \cdot n(B).$$

Na verdade, $n(A \times B) = n(A) \cdot n(B)$ para quaisquer conjuntos finitos A e B. O resultado segue da observação de que, para um par ordenado (a,b) em $A \times B$, existem $n(A)$ possibilidades para a e, para cada uma delas, existem $n(B)$ possibilidades para b.

A idéia de produto de conjuntos pode ser estendida para qualquer número finito de conjuntos. Para quaisquer conjuntos $A_1, A_2, \ldots, A_n$, o conjunto de todas as n-tuplas $(a_1, a_2, \ldots, a_n)$, onde $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$, é chamado de *produto* dos conjuntos $A_1, \ldots, A_n$ e é denotado por:

$$A_1 \times A_2 \times \cdots \times A_n \qquad \text{ou} \qquad \prod_{i=1}^{n} A_i .$$

Da mesma maneira que escrevemos A^2 em vez de $A \times A$, escrevemos A^n em vez de $A \times A \times \cdots \times A \times A$, onde existem n fatores, todos iguais a A. Por exemplo, $\mathbf{R}^3 = \mathbf{R} \times \mathbf{R} \times \mathbf{R}$ denota o espaço tridimensional usual.

2.3 RELAÇÕES

Começamos com uma definição:

Definição: Sejam A e B conjuntos. Uma *relação binária* ou, simplesmente, *relação* de A para B é um subconjunto de $A \times B$.

Suponha que R é uma relação de A para B. Então R é um conjunto de pares ordenados onde cada primeiro elemento pertence a A e cada segundo elemento pertence a B. Isto é, para cada par $a \in A$ e $b \in B$, exatamente uma das seguintes afirmativas é verdadeira:

(i) $(a,b) \in R$; dizemos que "a é R-*relacionado* a b", escrevendo $a\ R\ b$.

(ii) $(a,b) \notin R$; dizemos que "a não é R-relacionado a b", escrevendo $a \not R b$.

Se R é uma relação de um conjunto A para si mesmo, isto é, se R é um subconjunto de $A^2 = A \times A$, então dizemos que R é uma relação em A.

O *domínio* de uma relação R é o conjunto de todos os primeiro elementos de um par ordenado que pertence a R, e a imagem de R é o conjunto dos segundos elementos.

Embora as relações n-árias, que envolvem n-tuplas, sejam introduzidas na Seção 2.12, o termo "relação" significará relação binária, a menos que haja sentido implícito ou especificação em contrário.

Exemplo 2.3

(*a*) Sejam $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$, e seja $R = \{(1, y), (1, z) (3, y)\}$. Então R é uma relação de A para B, uma vez que R é um subconjunto de $A \times B$. Com respeito a esta relação,

$$1\,R\,y, \quad 1\,R\,z, \quad 3\,R\,y, \qquad \text{mas} \qquad 1 \not R x, \quad 2 \not R x, \quad 2 \not R y, \quad 2 \not R z, \quad 3 \not R x, \quad 3 \not R z .$$

O domínio de R é $\{1,3\}$ e a imagem é $\{y, z\}$.

(*b*) Sejam $A = \{\text{ovos, leite, milho}\}$ e $B = \{\text{vacas, cabras, galinhas}\}$. Podemos definir uma relação R de A para B por $(a,b) \in R$ se a é produzido por b. Em outras palavras,

$$R = \{(\text{ovos, galinhas}), (\text{leite, vacas}), (\text{leite, cabras})\}$$

De acordo com essa relação,

$$\text{ovos } R \text{ galinhas, leite } R \text{ vacas, etc.}$$

(*c*) Suponha que dois países são *adjacentes* se têm alguma parte de suas fronteiras em comum. Então, "ser adjacente a" é uma relação R definida nos países da Terra. Portanto,

$$(\text{Itália, Suíça}) \in R \text{ mas } (\text{Canadá, México}) \notin R.$$

(*d*) Inclusão de conjuntos, $\subseteq$, é uma relação em qualquer coleção de conjuntos. Na verdade, dado qualquer par de conjuntos A e B, então ou $A \subseteq B$ ou $A \not\subseteq B$.

(*e*) Uma relação comum no conjunto $\mathbf{Z}$ dos inteiros é "m divide n". Uma notação comum para essa relação é escrever $m|n$ quando m divide n. Portanto $6|30$, mas $7 \nmid 25$.

(*f*) Considere o conjunto L das retas no plano. Perpendicularidade, escrito $\perp$, é uma relação em L. Isto é, dado qualquer par de retas a e b, ou $a \perp b$ ou $a \not\perp b$. De maneira similar, "ser paralelo a", escrito $\|$, é uma relação em L já que $a \| b$ ou $a \nparallel b$.

(*g*) Seja A um conjunto qualquer. Uma relação importante em A é a relação de *igualdade*.

$$\{(a, a): a \in A\},$$

que é usualmente denotada por "=". Essa relação é também chamada de *identidade* ou *relação diagonal* em A e será também denotada por Δ_A ou Δ.

(*h*) Seja A um conjunto qualquer. Então $A \times A$ e $\varnothing$ são subconjuntos de $A \times A$ e, portanto, são relações em A denominadas, respectivamente, *relação universal* e *relação vazia*.

Relações Inversas

Seja R uma relação qualquer de um conjunto A para um conjunto B. A inversa de R, denotada por R^{-1}, é a relação de B para A que consiste nos pares ordenados que, quando têm sua ordem revertida, pertencem a R; isto é:

$$R^{-1} = \{(b, a): (a, b) \in R\}.$$

Por exemplo, a inversa da relação $R = \{(1, y), (1, z), (3, y)\}$ de A para B é a seguinte:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3)\}.$$

Claramente, se R é uma relação, então $(R^{-1})^{-1} = R$. Além disso, o domínio e a imagem de R^{-1} são, respectivamente, iguais à imagem e ao domínio de R. Ademais, se R é uma relação em A, então R^{-1} também é uma relação em A.

2.4 REPRESENTAÇÃO PICTÓRICA DE RELAÇÕES

Consideramos primeiramente uma relação S no conjunto $\mathbf{R}$ dos números reais; isto é, S é um subconjunto de $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$.

Como $\mathbf{R}^2$ pode ser representado pelo conjunto de pontos no plano, podemos representar S assinalando os pontos no plano que pertencem a S. A representação pictórica de S é geralmente chamada de *gráfico* da relação.

Freqüentemente a relação S consiste em todos os pares ordenados de números reais que satisfazem uma equação dada:

$$E(x, y) = 0.$$

Normalmente identificamos a relação com a equação, isto é, falamos da relação $E(x,y) = 0$.

Exemplo 2.4 Considere a relação S definida pela equação

$$x^2 + y^2 = 25.$$

Isto é, S consiste em todos os pares ordenados (x, y) que satisfazem a equação dada. O gráfico da equação é um círculo com centro na origem e raio 5. Veja a Figura 2-2.

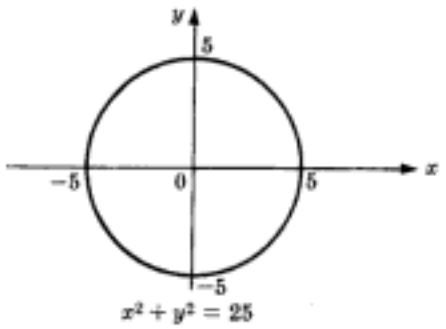


Fig. 2-2

Representações de Relações em Conjuntos Finitos

Suponha que A e B são conjuntos finitos. Apresentamos a seguir duas maneiras de representar graficamente uma relação R de A para B.

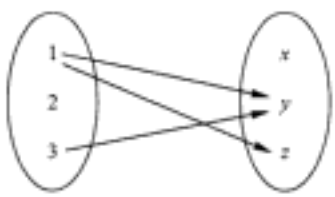
(i) Forme uma matriz retangular, nomeando as linhas pelos elementos de A e as colunas pelos elementos de B. Coloque 1 ou 0 em cada posição da matriz dependendo de $a \in A$ estar ou não relacionado com $b \in B$. Essa matriz é chamada de *matriz da relação*.

(ii) Escreva os elementos de A e os elementos de B em dois discos disjuntos e, então, desenhe uma seta de $a \in A$ para $b \in B$ sempre que a estiver relacionado com b.

A Figura 2-3 representa a primeira relação do Exemplo 2.3 das duas maneiras descritas acima.

	x	y	z
1	0	1	1
2	0	0	0
3	0	1	0

(i)



(ii)

$R = \{(1, y), (1, z), (3, y)\}$

Fig. 2-3

Grafos Orientados em Relações de Conjuntos

Existe uma outra maneira de representar graficamente uma relação R quando R é uma relação de um conjunto finito nele mesmo. Primeiramente escrevemos os elementos do conjunto e então desenhamos uma seta de cada elemento x para um elemento y sempre que x estiver relacionado a y. Esse diagrama é denominado *grafo orientado* da relação. A Figura 2-4, por exemplo, mostra o grafo orientado da seguinte relação R no conjunto $A = \{1, 2, 3, 4\}$:

$$R = \{(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)\}.$$

Observe que existe uma seta partindo de 2 para si mesmo, já que 2 está relacionado a 2 por R.

Esses grafos orientados serão estudados em detalhes, como um tema separado, no Capítulo 8. Eles estão mencionados aqui principalmente para que se dê tratamento completo ao assunto.

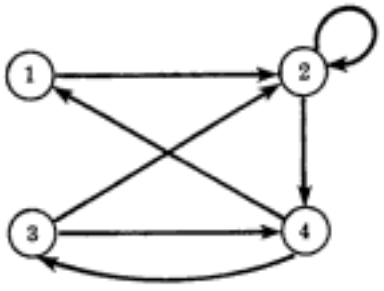


Fig. 2-4

2.5 COMPOSIÇÃO DE RELAÇÕES

Sejam A, B e C conjuntos, e seja R uma relação de A para B e seja S uma relação de B para C. Isto é, R é um subconjunto de $A \times B$, e S é um subconjunto de $B \times C$. Então R e S originam uma relação de A para C denotada por $R \circ S$ e definida por:

$$a(R \circ S)c \text{ se para algum } b \in B \text{ temos } aRb \text{ e } bSc.$$

Isto é,

$$R \circ S = \{(a,c): \text{existe } b \in B \text{ para o qual } (a, b) \in R \text{ e } (b, c) \in S\}.$$

A relação $R \circ S$ é dita a *composição* de R e S; é algumas vezes denotada simplesmente por RS.

Suponha que R é uma relação em um conjunto A, isto é, R é uma relação de A para ele mesmo. Então $R \circ R$, isto é, a composição de R com ela mesma está sempre definida, e $R \circ R$ é às vezes denotada por R^2. Analogamente, $R^3 = R^2 \circ R = R \circ R \circ R$, e assim por diante. Portanto, R^n é definida para todo n positivo.

Aviso: Muitos textos denotam a composição de relações R e S por $S \circ R$. Isso é feito para obter compatibilidade com a notação usual de $g \circ f$ para denotar a composição de f e g onde f e g são funções. Portanto, o leitor pode ter de ajustar sua notação quando usar este texto como complementar de outro. Entretanto, quando uma relação R é composta com ela mesma, o significado de $R \circ R$ não apresenta ambigüidades.

O diagrama de setas da relação nos dá uma interpretação geométrica da composição $R \circ S$ como se vê no exemplo seguinte.

Exemplo 2.5 Sejam $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, $C = \{x, y, z\}$ e seja

$$R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\} \text{ e } S = \{(b, x), (b, z), (c, y), (d, z)\}.$$

Considere o diagrama de setas de R e S como na Figura 2-5. Observe que existe uma seta de 2 para d que é seguida por uma seta de d para z. Podemos considerar essas duas setas como um caminho que conecta o elemento $2 \in A$ ao elemento $z \in C$. Portanto,

$$2(R \circ S)z \qquad \text{já que} \qquad 2Rd \text{ e } dSz$$

De maneira similar, existe um caminho de 3 para x e um caminho de 3 para z. Portanto,

$$3(R \circ S)x \quad \text{e} \quad 3(R \circ S)z,$$

Nenhum outro elemento de A está conectado a um elemento de C. Conseqüentemente,

$$R \circ S = \{(2, z), (3, x), (3, z)\}$$

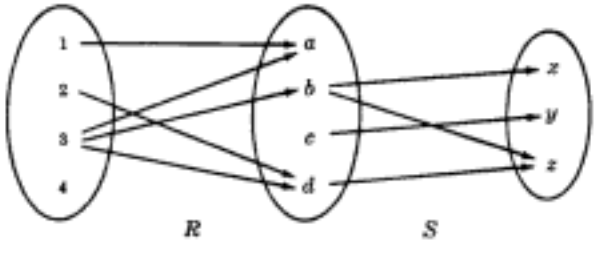


Fig. 2-5

Composição de Relações e Matrizes

Existe uma outra maneira de determinar $R \circ S$. Sejam M_R e M_S, respectivamente, as matrizes da relação R e S. Então,

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \qquad \text{e} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Multiplicando M_R e M_S, obtemos a matriz

$$M = M_R M_S = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Os elementos não nulos dessa matriz nos mostram quais elementos estão relacionados por $R \circ S$. Portanto, $M = M_R M_S$ e $M_{R \circ S}$ têm os mesmos elementos não nulos.

Nosso primeiro teorema diz que a composição de relações é associativa.

Teorema 2-1: sejam A, B, C e D conjuntos. Suponha que R é uma relação de A para B, S é uma relação de B para C e T é uma relação de C para D. Então,

$$(R \circ S) \circ T = R \circ (S \circ T).$$

Provamos esse teorema no Problema 2.11.

2.6 TIPOS DE RELAÇÕES

Considere um dado conjunto A. Esta seção discute tipos de relações importantes que estão definidas em A.

Relações Reflexivas

Uma relação R em um conjunto A é reflexiva se aRa para todo $a \in A$, isto é, se $(a, a) \in R$ para todo $a \in A$. Portanto, R não é reflexiva se existe um $a \in A$ tal que $(a,a) \notin$ R.

Exemplo 2.6 Considere as seguintes cinco relações em um conjunto $A = [1, 2, 3, 4]$:

$$\begin{aligned} R_1 &= \{(1,1), (1,2), (2,3), (1,3), (4,4)\}; \\ R_2 &= \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}; \\ R_3 &= \{(1,3), (2,1)\}; \\ R_4 &= \varnothing, \text{ a relação vazia}; \\ R_5 &= A \times A, \text{ a relação universal}. \end{aligned}$$

Determine quais das relações são reflexivas.

Como A contém os quatro elementos 1, 2, 3 e 4, uma relação R em A é reflexiva se contém os quatro pares (1,1), (2,2), (3,3) e (4,4). Portanto, apenas R_2 e a relação universal $R_5 = A \times A$ são reflexivas. Note que R_1, R_3 e R_4 não são reflexivas uma vez que, por exemplo, (2, 2) não pertence a nenhuma delas.

Exemplo 2.7 Considere as seguintes cinco relações:

(1) Relação $\leq$ (menor ou igual) no conjunto $\mathbf{Z}$ dos inteiros.
(2) Inclusão de conjuntos $\subseteq$ numa coleção $\mathcal{C}$ de conjuntos.
(3) Relação $\perp$ (perpendicularidade) em um conjunto L de retas no plano.
(4) Relação $\parallel$ (paralelismo) em um conjunto L de retas no plano.
(5) Relação $|$ de divisibilidade no conjunto $\mathbf{N}$ de inteiros positivos. (Lembre que $x|y$ se existe um z tal que $xz = y$.)

Determine quais das relações são reflexivas.

A relação (3) não é reflexiva já que nenhuma reta é perpendicular a si mesma. Também (4) não é reflexiva já que nenhuma reta é paralela a si mesma. As outras relações são reflexivas; isto é, $x \leq x$ para todo inteiro $x \in \mathbf{Z}$, $A \subseteq A$ para todo $A \in \mathcal{C}$ e $n|n$ para todo inteiro positivo $n \in \mathbf{N}$.

Relações Simétricas e Anti-simétricas

Uma relação R em um conjunto A é *simétrica* se aRb implica bRa, isto é, se $(a,b) \in R$ implica $(b,a) \in R$. Logo, R não é simétrica se existe $(a,b) \in R$, mas $(b,a) \notin R$.

Exemplo 2.8

(*a*) Determine quais das relações do Exemplo 2-6 são simétricas.

R_1 não é simétrica já que $(1, 2) \in R_1$ mas $(2, 1) \notin R_1$. R_3 não é simétrica já que $(1,3) \in R_3$ mas $(3,1) \notin R_3$. As outras relações são simétricas.

(*b*) Determine quais das relações no Exemplo 2-7 são simétricas.

A relação R é simétrica, pois, se a reta a é perpendicular à reta b, então b é perpendicular à a. Além disso, a relação $\|$ é simétrica já que, se a reta a é paralela à reta b, então b é paralela à a. As outras relações não são simétricas. Por exemplo, $3 \leq 4$, mas $4 \not\leq 3$; $\{1, 2\} \subseteq \{1, 2, 3\}$, mas $\{1, 2, 3\} \not\subseteq \{1, 2\}$; e $2|6$, mas $6 \not| 2$.

Uma relação R em um conjunto A é *anti-simétrica* se aRb e bRa implica $a=b$, isto é, se (a,b) e $(b,a) \in R$, então, $a = b$. Portanto, R não é anti-simétrica se existem $a, b \in A$ tais que (a,b) e $(b,a) \in R$, mas $a \neq b$.

Exemplo 2.9

(*a*) Determine quais das relações do Exemplo 2-6 são anti-simétricas.

R_2 não é anti-simétrica, já que $(1,2)$ e $(2,1)$ pertencem a R_2, mas $1 \neq 2$. Analogamente, a relação universal R_5 não é anti-simétrica. Todas as outras relações são anti-simétricas.

(*b*) Determine quais das relações no Exemplo 2-7 são anti-simétricas.

A relação $\leq$ é anti-simétrica pois, sempre que $a \leq b$ e $b \leq a$, então $a = b$. A inclusão de conjuntos é anti-simétrica já que, sempre que $A \subseteq B$ e $B \subseteq A$, então $A = B$. Além disso, a divisibilidade em $\mathbf{N}$ é anti-simétrica já que $m|n$ e $n|m$, então $m = n$. (Note que a divisibilidade em $\mathbf{Z}$ não é anti-simétrica uma vez que $3|-3$ e $-3|3$, mas $3 \neq -3$.) A relação $\perp$ não é anti-simétrica já que se pode ter retas distintas a e b tais que $a \perp b$ e $b \perp a$. Similarmente, $\|$ não é anti-simétrica.

Observação: As propriedades de simetria e anti-simetria não são mutuamente excludentes. Por exemplo, a relação $R = \{(1, 3), (3, 1), (2, 3)\}$ não é nem simétrica nem anti-simétrica. Por outro lado, a relação $R' = \{(1, 1), (2, 2)\}$ é simétrica e anti-simétrica.

Relações Transitivas

Uma relação R em um conjunto A é *transitiva* se aRb e bRc implica aRc, isto é, se (a,b) e $(b,a) \in R$, então $(a,c) \in R$. Logo, R não é transitiva se existem $a, b, c \in$ A tais que (a,b) e $(b,c) \in R$, mas $(a,c) \notin R$.

Exemplo 2.10

(*a*) Determine quais das relações no Exemplo 2.6 são transitivas.

A relação R_3 não é transitiva porque $(2,1)$ e $(1,3) \in R_3$, mas $(2,3) \notin R_3$. Todas as outras relações são transitivas.

(*b*) Determine quais das relações no Exemplo 2.7 são transitivas.

As relações $\leq$, $\subseteq$ e $|$ são transitivas. Isto é, (i) $a \leq b$ e $b \leq c$ então, $a \leq c$. (ii) Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$. (iii) Se $a|b$ e $b|c$, então $a|c$.

Por outro lado, a relação $\perp$ não é transitiva. Se $a \perp b$ e $b \perp c$, então não é verdade que $a \perp b$. Como nenhuma reta é paralela a si mesma, podemos ter $a \| b$ e $b \| a$, mas $a \not\| a$. Portanto, $\|$ não é transitiva. (Notamos que a relação "ser paralelo ou igual a" é uma relação transitiva no conjunto L das retas no plano.)

A propriedade de transitividade também pode ser expressa em termos da composição de relações. Para uma relação R em A, definimos

$$R^2 = R \circ R \qquad \text{e, mais geralmente,} \qquad R^n = R^{n-1} \circ R.$$

Então, temos o seguinte resultado.

Teorema 2-2: a relação R é transitiva se e somente se $R^n \subseteq R$ para $n \geq 1$.

2.7 PROPRIEDADES DE FECHO

Considere um conjunto A e a coleção de todas as relações em A. Seja P uma propriedade dessas relações, tal como simetria ou transitividade. Uma relação com a propriedade P será chamada de uma P-relação. O P-fecho de uma relação arbitrária R em A, denotado $P(R)$, é uma P-relação tal que

$$R \subseteq P(R) \subseteq S$$

para toda P-relação S contendo R. Usaremos a notação

$$\text{reflexivo}(R),\ \text{simétrico}(R) \text{ e } \text{transitivo}(R)$$

para os fechos reflexivo, simétrico e transitivo de R.

De um modo geral, $P(R)$ não precisa existir. Entretanto, existe uma situação geral em que $P(R)$ sempre existirá. Suponha que P seja uma propriedade tal que existe pelo menos uma P-relação contendo R, e que a interseção de quaisquer P-relações seja também uma P-relação. Então, é possível provar (Problema 2.16) que

$$P(R) = \cap(S:\ S \text{ é uma } \boldsymbol{P}\text{-relação e } R \subseteq S).$$

Logo, pode-se obter $P(R)$ a partir de "restrições"†, isto é, a partir da interseção de relações. Entretanto, é freqüente que se queira determinar $P(R)$ a partir de "ampliações"††, isto é, acrescentando elementos a R para obter $P(R)$. Executamos isso abaixo.

Fechos Reflexivos e Simétricos

O próximo teorema nos diz como é fácil obter os fechos reflexivo e simétrico de uma relação.

Teorema 2-3: seja R uma relação em um conjunto A. Então:

(i) $R \cup \Delta_A$ é o fecho reflexivo de R.

(ii) $R \cup R^{-1}$ é o fecho simétrico de R.

Em outras palavras, reflexivo(R) é obtido simplesmente adicionando a R os elementos (a,a) da diagonal que não pertencem originalmente a R, e simétrico(R) é obtido por adicionar a R todos os pares (b,a) tais que (a,b) pertence a R.

Exemplo 2.11

(*a*) Considere a seguinte relação R no conjunto $A = \{1,2,3,4\}$:

$$R = \{(1,1),\ (1,3),\ (2,4),\ (3,1),\ (3,3),\ (4,3)\}.$$

Então:

$$\text{reflexivo}(R) = R \cup \{(2,2),\ (4,4)\} \qquad \text{e simétrico}(R) = R \cup \{(4,2),\ (3,4)\}.$$

(*b*) Considere a relação $<$ (menor do que) no conjunto $\mathbf{N}$ dos inteiros positivos. Então,

$$\text{reflexivo}(<) = < \cup \Delta = \leq = \{(a,b):\ a \leq b\}$$

$$\text{simétrico}(<) = < \cup > = \{(a,b):\ a \neq b\}$$

Fecho Transitivo

Seja R uma relação em um conjunto A. Lembre que $R^2 = R \circ R$ e $R^n = R^{n-1} \circ R$. Definimos

$$R^* = \bigcup_{i=1}^{\infty} R^i.$$

† N. de T. No original, *from the top-down*.

†† N. de T. No original, *from the bottom-up*.

Vale o teorema a seguir.

Teorema 2-4: R^* é o fecho transitivo da relação R.

Suponha que A é um conjunto finito com n elementos. Então, mostramos no Capítulo 8, sobre grafos orientados, que

$$R^* = R \cup R^2 \cup \cdots \cup R^n$$

Obtemos, do teorema acima, o seguinte resultado.

Teorema 2-5: seja R uma relação em um conjunto A com n elementos. Então.

$$\text{transitivo}(R) = R \cup R^2 \cup \cdots \cup R^n$$

Achar transitivo(R) pode tomar muito tempo quando A tem um grande número de elementos. Uma maneira eficiente de fazer isso será descrita no Capítulo 8. Apresentamos aqui um exemplo simples em que A tem apenas três elementos.

Exemplo 2.12 Considere a seguinte relação R em $A = \{1, 2, 3\}$:

$$R = \{(1,2), (2,3), (3,3)\}$$

Então,

$$R^2 = R \circ R = \{(1,3), (2,3)(3,3)\} \qquad \text{e} \qquad R^3 = R^2 \circ R = \{(1,3), (2,3), (3,3)\}$$

Coerentemente,

$$\text{transitivo}(R) = R \cup R^2 \cup R^3 = \{(1,2), (2,3), (3,3), (1,3)\}$$

2.8 RELAÇÕES DE EQUIVALÊNCIA

Considere um conjunto não vazio S. Uma relação R em S é uma *relação de equivalência* se R é reflexiva, simétrica e transitiva. Isto é, R é uma relação de equivalência em S se tem as seguintes três propriedades:

(1) Para todo $a \in S$, aRa.

(2) Se aRb, então bRa.

(3) Se aRb e bRc, então aRc.

A idéia geral subjacente à de relação de equivalência é de que ela é uma classificação de objetos que, em algum sentido, são parecidos. Na verdade, a relação "=" de igualdade, em qualquer conjunto S, é uma relação de equivalência; isto é:

(1) $a=a$ para todo $a \in S$.

(2) Se $a=b$, então $b=a$.

(3) Se $a=b$ e $b=c$, então $a=c$.

Apresentamos outras relações de equivalência a seguir.

Exemplo 2.13

(*a*) Considere o conjunto L das retas e o conjunto T dos triângulos no espaço euclidiano. A relação "é paralelo a ou é igual a" é uma relação de equivalência em L, e congruência e similaridade são relações de equivalência em T.

(*b*) A classificação de animais em espécies, isto é, a relação "é da mesma espécie que" é uma relação de equivalência no conjunto de animais.

(*c*) A relação $\subseteq$ de inclusão de conjuntos não é uma relação de equivalência. É reflexiva e transitiva, mas não é simétrica, já que $A \subseteq B$ não implica $B \subseteq A$.

(*d*) Seja m um inteiro fixo positivo. Dois inteiros a e b são ditos *congruentes módulo m*, denotado

$$a \equiv b \pmod{m},$$

se m divide $a - b$. Por exemplo, para $m = 4$, temos $11 \equiv 3 \pmod 4$ já que 4 divide $11 - 3$, e $22 \equiv 6 \pmod 4$ já que 4 divide $22 - 6$. A relação de congruência módulo m é uma relação de equivalência.

Relações de Equivalência e Partições

Esta seção explora a ligação entre relações de equivalência e partições em um conjunto não vazio S. Lembre primeiramente que uma partição P de S é uma coleção $\{A_i\}$ de conjuntos não vazios de S com as duas propriedades seguintes:

(1) Cada $a \in S$ pertence a algum A_i.

(2) Se $A_i \neq A_j$, então $A_i \cap A_j = \varnothing$.

Em outras palavras, uma partição P de S é uma subdivisão de S em conjuntos disjuntos não vazios. (Veja a Seção 1.9-4).

Suponha que R seja uma relação de equivalência em um conjunto S. Para cada $a \in S$, denote por $[a]$ o conjunto de elementos de S aos quais a está relacionado por R; isto é,

$$[a] = \{x: (a, x) \in R\}.$$

Chamamos de $[a]$ a classe de equivalência de a em S; qualquer $b \in [a]$ é dito *representante* da classe de equivalência.

A coleção de todas as classe de equivalência de elementos de S por uma relação de equivalência R é denotada por S/R, isto é,

$$S/R = \{[a]: a \in S\}$$

é chamado de conjunto *quociente* de S por R. A propriedade fundamental de um conjunto quociente está contida no teorema seguinte.

Teorema 2-6: seja R uma relação de equivalência em um conjunto S. O quociente S/A é uma partição de S. Especificamente:

(i) Para cada $a \in S$, temos $a \in [a]$.
(ii) $[a] = [b]$ se e somente se $(a,b) \in R$.
(iii) Se $[a] \neq [b]$, então $[a]$ e $[b]$ são disjuntos.

Por outro lado, dada uma partição $\{A_i\}$ do conjunto S, existe uma relação de equivalência R em S tal que os conjuntos A_i são as classes de equivalência.

Esse importante teorema será provado no Problema 2.21.

Exemplo 2.14

(*a*) Considere a seguinte relação R em $S = \{1, 2, 3\}$:

$$R = \{(1,1), (1,2), (2,1), (2,2), (3,3)\}.$$

É possível mostrar que R é reflexiva, simétrica e transitiva, isto é, R é uma relação de equivalência. Sob a relação R,

$$[1] = \{1, 2\}, \qquad [2] = \{1, 2\}, \qquad [3] = \{3\}.$$

Observe que $[1] = [2]$ e que $S/R = \{[1],[3]\}$ é uma partição de S. Pode-se escolher $\{1, 3\}$ ou $\{2, 3\}$ como conjunto de representantes das classes de equivalência.

(*b*) Seja R_5 a relação no conjunto $\mathbf{Z}$ de inteiros definida por

$$x \equiv y \pmod 5.$$

que se lê "x é congruente a y módulo 5" e que significa que a diferença $x - y$ é divisível por 5. Então, R_5 é uma relação de equivalência em $\mathbf{Z}$. Existem exatamente cinco classes de equivalência no conjunto quociente $\mathbf{Z}/R_5$ como a seguir:

$$A_0 = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$A_1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$A_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$A_3 = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$A_4 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$

Observe que qualquer inteiro x, que pode ser expresso de maneira única como $x = 5q + r$ onde $0 \le r < 5$, é um elemento da classe de equivalência A_r onde r é o resto. Como esperado, as classes de equivalência são disjuntas e

$$\mathbf{Z} = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 .$$

Usualmente se escolhe $\{0, 1, 2, 3, 4\}$ ou $\{-2, -1, 0, 1, 2\}$ como conjunto de representantes das classes de equivalência.

2.9 RELAÇÕES DE ORDEM PARCIAL

Esta seção define uma outra classe importante de relações. Uma relação R em um conjunto S é dita um *ordenamento parcial* ou *uma ordem parcial* se R é reflexiva, anti-simétrica e transitiva. Um conjunto S, juntamente com uma ordem parcial R, é dito *parcialmente ordenado*[†]. Conjuntos parcialmente ordenados serão estudados com mais detalhes no Capítulo 14, de forma que aqui apenas apresentamos alguns exemplos.

Exemplo 2.15

(*a*) A relação $\subseteq$ de inclusão de conjuntos é uma ordem parcial em qualquer coleção de conjuntos, uma vez que inclusão de conjuntos tem as três propriedades desejadas. Isto é,

(1) $A \subseteq A$ para todo conjunto A.
(2) Se $A \subseteq B$ e $B \subseteq A$, então $A = B$
(3) Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(*b*) A relação $\le$ no conjunto $\mathbf{R}$ dos números reais é reflexiva, anti-simétrica e transitiva. Portanto, $\le$ é uma relação de ordem parcial.

(*c*) A relação "a divide b" é uma relação de ordem parcial no conjunto $\mathbf{N}$ de inteiros positivos. Entretanto "a divide b" não é uma relação de ordem parcial no conjunto $\mathbf{Z}$ dos inteiros, já que $a|b$ e $b|a$ não implica $a=b$. Por exemplo, $3|-3$ e $-3|3$ mas $3 \ne -3$.

2.10 RELAÇÕES *N*-ÁRIAS

Todas as relações discutidas anteriormente eram relações binárias. Uma *relação n-ária* é um conjunto de n-tuplas. Para todo conjunto S, um subconjunto do conjunto produto S^n é dito uma relação n-ária em S. Em particular, um subconjunto de S^3 é dito uma *relação ternária* em S.

Exemplo 2.16

(*a*) Seja L uma reta no plano. A "interposição"[††] é uma relação ternária R nos pontos de L; isto é, $(a, b, c) \in R$ se b estiver entre a e c em L.

(*b*) A equação $x^2 + y^2 + z^2 = 1$ determina a relação ternária T no conjunto $\mathbf{R}$ dos números reais. Isto é, a tripla (x,y,z) pertence a T se (x,y,z) satisfaz a equação, o que significa que (x,y,z) são as coordenadas de um ponto em $\mathbf{R}^3$ na esfera S com raio 1 e centro na origem $O = (0, 0, 0)$.

Problemas Resolvidos

Pares Ordenados e Produtos de Conjuntos

2.1 Dados $A = \{1, 2, 3\}$ e $B = \{a, b\}$, ache (*a*) $A \times B$; (*b*) $B \times A$; (*c*) $B \times B$.

(*a*) $A \times B$ consiste em todos os pares ordenados (x, y), onde $x \in A$ e $y \in B$. Assim,

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

(*b*) $B \times A$ consiste em todos os pares ordenados (y, x), onde $y \in B$ e $x \in A$. Logo,

$$B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}.$$

[†] N. de T. No original, também abreviado como *poset*, referente a *partially ordered set*.

[††] N. de T. No original, *betweenness*.

(*c*) $B \times B$ consiste em todos os pares ordenados (x, y), onde $x, y \in B$. Portanto,

$$B \times B = \{(a,a), (a,b), (b,a), (b,b)\}.$$

Como esperado, o número de elementos no conjunto produto é igual ao produto do número de elementos em cada conjunto.

2.2 Dados $A = \{1, 2\}$, $B = \{(x, y, z)\}$ e $C = \{3, 4\}$, ache $A \times B \times C$.

$A \times B \times C$ consiste em todas as triplas ordenadas (a, b, c) onde $a \in A$, $b \in B$, $c \in C$. Esses elementos de $A \times B \times C$ podem ser sistematicamente obtidos pelo conhecido diagrama de árvore (Figura 2-6). Os elementos de $A \times B \times C$ são precisamente as 12 triplas ordenadas à direita do diagrama de árvore.

Observe que $n(A) = 2$, $n(B) = 3$, $n(C) = 2$ e, como esperado,

$$n(A \times B \times C) = 12 = n(A) \cdot n(B) \cdot n(C)$$

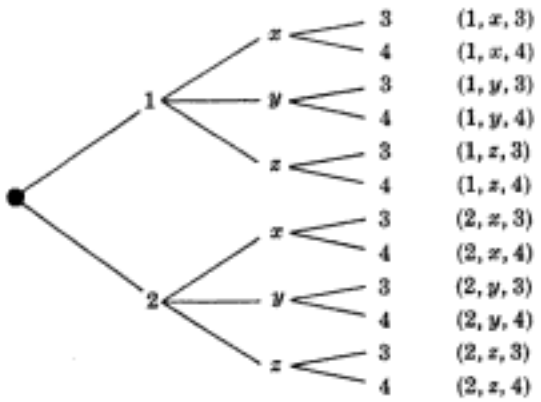


Fig. 2-6

2.3 Sejam $A = \{1, 2\}$, $B = \{a, b, c\}$ e $C = \{c, d\}$. Ache $(A \times B) \cap (A \times C)$ e $(B \cap C)$.

Temos

$$A \times B = \{(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)\}$$
$$A \times C = \{(1,c), (1,d), (2,c), (2,d)\}$$

Portanto,

$$(A \times B) \cap (A \times C) = \{(1,c), (2,c)\}.$$

Como $B \cap C = \{c\}$,

$$A \times (B \cap C) = \{(1,c), (2,c)\}.$$

Observe que $(A \times B) \cap (A \times C) = A \times (B \cap C)$. Esse fato é verdadeiro para quaisquer conjuntos A, B e C (veja o Problema 2.4).

2.4 Mostre que $(A \times B) \cap (A \times C) = A \times (B \cap C)$.

$$\begin{aligned}(A \times B) \cap (A \times C) &= \{x,y)\colon (x,y) \in A \times B \text{ e } (x,y) \in A \times C\} \\ &= \{(x,y)\colon x \in A, y \in B \text{ e } x \in A, y \in C\} \\ &= \{(x,y)\colon x \in A, y \in B \cap C\} \quad = \quad A \times (B \cap C)\end{aligned}$$

2.5 Ache x e y, dado $(2x, x + y) = (6, 2)$.

Dois pares ordenados são iguais se e somente se os componentes correspondentes são iguais. Portanto, obtemos as equações

$$2x = 6 \quad \text{e} \quad x + y = 2,$$

para as quais deduzimos as respostas $x = 3$ e $y = -1$.

Relações e seus Grafos

2.6 Ache o número de relações de $A = \{a, b, c\}$ para $B = \{1, 2\}$.

Existem $3(2) = 6$ elementos em $A \times B$ e, portanto, existem $m = 2^6 = 64$ subconjuntos de $A \times B$. Logo existem $m = 64$ relações de A para B.

2.7 São dados $A = \{1, 2, 3, 4\}$ e $B = \{x, y, z\}$. Seja R a seguinte relação de A para B:

$$R = \{(1, y), (1, z), (3, y), (4, x), (4, z)\}.$$

(*a*) Determine a matriz da relação. (*b*) Desenhe o diagrama de setas de R. (*c*) Ache a relação inversa R^{-1} de R. (*d*) Determine o domínio e a imagem de R.

(*a*) Veja a Figura 2-7(*a*). Observe que as linhas da matriz estão designadas pelos elementos de A, e as colunas pelos elementos de B. Observe também que o elemento na matriz que corresponde a $a \in A$ e $b \in B$ é 1 se a estiver relacionado com b e 0 caso contrário.

(*b*) Veja Figura 2-7(*b*). Observe que existe uma seta de $a \in A$ para $b \in B$ se e somente se a estiver relacionado a b, i.e., se e somente se $(a, b) \in R$.

(*c*) Reverta a ordem dos pares de R para obter R^{-1}:

$$R^{-1} = \{(y, 1), (z, 1), (y, 3), (x, 4), (z, 4)\}.$$

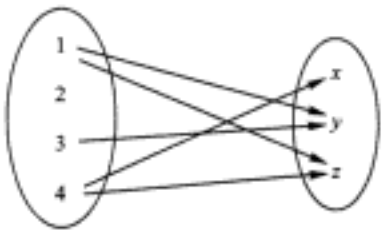
Observe que, revertendo as setas na Figura 2-7(*b*), obtemos o diagrama de setas de R^{-1}.

(*d*) O Domínio de R, Dom(R), dos primeiros elementos dos pares ordenados de R, e a Imagem de R, Ran(R)[†], consiste nos segundos elementos. Logo,

$$\text{Dom}(R) = \{1, 3, 4\} \qquad \text{e} \qquad \text{Ran}(R) = \{x, y, z\}$$

$$\begin{array}{c|ccc} & x & y & x \\ 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{array}$$

(*a*)



(*b*)

Fig. 2-7

2.8 Seja $A = \{1, 2, 3, 4, 6\}$ e seja R a relação em A definida por "x divide y", escrita $x|y$. (Note que $x|y$ se e somente se existe algum inteiro z tal que $xz = y$.)
(*a*) Escreva R como um conjunto de pares ordenados. (*b*) Desenhe seu grafo orientado. (*c*) Ache a relação inversa R^{-1} de R. R^{-1} pode ser descrita em palavras?

(*a*) Ache os números em A divisíveis por 1, 2, 3, 4 e, depois, 6. São eles:

$$1|1, \quad 1|2, \quad 1|3, \quad 1|4, \quad 1|6, \quad 2|2, \quad 2|4, \quad 2|6, \quad 3|3, \quad 3|6, \quad 4|4, \quad 6|6$$

Portanto,

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}$$

(*b*) Veja a Figura 2-8.

(*c*) Reverta a ordem dos pares ordenados de R para obter R^{-1}:

[†] N. de T. Do inglês, *Range*(R). A abreviatura Ran(R) é bastante usada em textos redigidos em português; alguns autores utilizam Im(R).

$$R^{-1} = \{(1,1),(2,1),(3,1),(4,1),(6,1),(2,2),(4,2),(6,2),(3,3),(6,3),(4,4),(6,6)\}.$$

R^{-1} pode ser descrito pela declaração "x é um múltiplo de y".

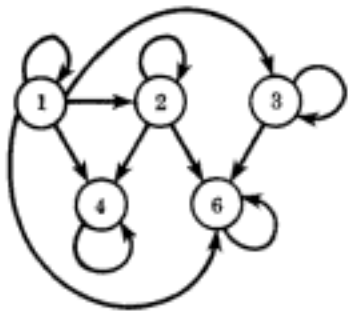


Fig. 2-8

2.9 Sejam $A = \{1, 2, 3\}$, $B = \{a, b, c\}$ e $C = \{x, y, z\}$. Considere as seguintes relações R e S de A para B e de B para C, respectivamente:

$$R = \{(1,b),(2,a),(2,c)\} \qquad \text{e} \qquad S = \{(a,y),(b,x),(c,y),(c,z)\}.$$

(*a*) Ache a relação composta $R \circ S$.

(*b*) Ache as matrizes M_R, M_S e $M_{R\circ S}$ das respectivas relações R, S e $R \circ S$ e compare $M_{R\circ S}$ ao produto $M_R M_S$.

(*a*) Desenhe o diagrama de setas das relações R e S como na Figura 2-9. Observe que A está "conectado" a x em C pelo caminho $1 \to b \to x$; portando $(1,x)$ pertence a $R \circ S$. De maneira similar, $(2, y)$ e $(2, z)$ pertencem a $R \circ S$. Temos

$$R \circ S = \{(1,x),(2,y),(2,z)\}.$$

(Veja o Exemplo 2.5.)

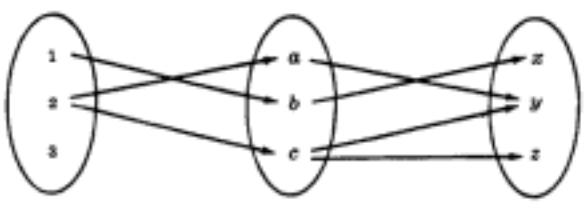


Fig. 2-9

(*b*) As matrizes M_R, M_S e $M_{R\circ S}$ são:

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array} \qquad M_S = \begin{array}{c} \\ a \\ b \\ c \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \qquad M_{R\circ S} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

Multiplicando M_R e M_S, obtemos

$$M_R M_S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Observe que $M_{R\circ S}$ e $M_R M_S$ têm os mesmos elementos nulos.

2.10 Sejam R e S as seguintes relações em $A = \{1, 2, 3\}$:

$$R = \{(1,1),(1,2),(2,3),(3,1),(3,3)\}, \qquad S = \{(1,2),(1,3),(2,1),(3,3)\}.$$

Ache (*a*) $R \cap S, R \cup S, R^c$; (*b*) $R \circ S$; (*c*) $S^2 = S \circ S$.

(*a*) Trate R e S simplesmente como conjuntos e faça a interseção e a união usuais. Para R^c, use o fato de que $A \times A$ é a relação universal em A.

$$R \cap S = \{(1,2),(3,3)\}$$
$$R \cup S = \{(1,1),(1,2),(1,3),(2,1),(2,3),(3,1),(3,3)\}$$
$$R^c = \{(1,3),(2,1),(2,2),(3,2)\}$$

(*b*) Para cada par $(a,b) \in R$, ache os pares $(b,c) \in S$. Então $(a,c) \in R \circ S$. Por exemplo, $(1, 1) \in R$ e $(1, 2), (1, 3) \in S$; portanto, (1, 2) e (1, 3) pertencem a $R \circ S$. Logo,

$$R \circ S = \{(1,2),(1,3),(1,1),(2,3),(3,2),(3,3)\}$$

(*c*) Seguindo o algoritmo em (*b*), obtemos:

$$S^2 = S \circ S = \{(1,1),(1,3),(2,2),(2,3),(3,3)\}$$

2.11 Prove o Teorema 2.1: sejam A, B, C e D conjuntos. Suponha que R seja uma relação de A para B, S seja uma relação de B para C e T seja uma relação de C para D. Então, $(R \circ S) \circ T = R \circ (S \circ T)$.

Precisamos mostrar que cada par ordenado em $(R \circ S) \circ T$ pertence a $R \circ (S \circ T)$ e vice-versa.

Suponha (a,d) pertence a $(R \circ S) \circ T$. Então, existe um c em C tal que $(a, c) \in R \circ S$ e $(c, d) \in T$. Como $(a, c) \in R \circ S$, existe b em B tal que $(a, b) \in R$ e $(b, c) \in S$. Como $(b, c) \in S$ e $(c, d) \in T$, temos $(b, d) \in S \circ T$; como $(a, b) \in R$ e (b, d) e $S \circ T$, temos $(a, d) \in R \circ (S \circ T)$. Portanto, $(R \circ S) \circ T \subseteq R \circ (S \circ T)$. De modo similar, $R \circ (S \circ T) \subseteq (R \circ S) \circ T$. Ambas as inclusões provam que $(R \circ S) \circ T = R \circ (S \circ T)$.

Tipos de Relações e Propriedades de Fecho

2.12 Considere as seguintes cinco relações em um conjunto $A = \{1, 2, 3\}$:

$$R = \{(1,1),(1,2),(1,3),(3,3)\} \qquad \varnothing = \text{relação vazia}$$
$$S = \{(1,1),(1,2),(2,1),(2,2),(3,3)\} \qquad A \times A = \text{relação universal}$$
$$T = \{(1,1),(1,2),(2,2),(2,3)\}$$

Determine se as relações acima em A são (*a*) reflexivas, (*b*) simétricas, (*c*) transitivas, (*d*) anti-simétricas.

(*a*) R não é reflexiva já que $2 \in A$, mas $(2, 2) \notin R$. T não é reflexiva já que $(3, 3) \notin T$ e, de modo similar, $\varnothing$ não é reflexiva. S e $A \times A$ são reflexivas.

(*b*) R não é simétrica já que $(1, 2) \in R$, mas $(2, 1) \notin R$ e, de modo similar, T não é simétrica. S, $\varnothing$ e $A \times A$ são simétricas.

(*c*) T não é transitiva já que (1, 2) e (2, 3) pertencem a T, mas $(1, 3) \notin T$. As outras quatro relações são transitivas.

(*d*) S não é anti-simétrica já que $1 \neq 2$ e ambos (1, 2) e (2, 1) pertencem a S. De forma similar, $A \times A$ não é anti-simétrica. As outras três relações são anti-simétricas.

2.13 Seja $A = \{1, 2, 3, 4\}$. Considere a seguinte relação em A.

$$R = \{(1,1),(2,2),(2,3),(3,2),(4,2),(4,4)\}.$$

(*a*) Desenhe seu grafo orientado. (*b*) R é (i) reflexiva, (ii) simétrica, (iii) transitiva ou (iv) anti-simétrica? (*c*) Ache $R^2 = R \circ R$.

(*a*) Veja a Figura 2-10.

(*b*) (i) R não é reflexiva porque $3 \in A$, mas $3 \not R 3$, i. e., $(3,3) \notin R$.

(ii) R não é simétrica porque $4R2$, mas $2\not R4$, i. e.,$(4,2) \in R$, mas $(2,4) \notin R$.

(iii) R não é transitiva porque $4R2$ e $2R3$ mas $4\not R3$, i.e.,$(4,2) \in R$ e $(2,3) \in R$, mas $(4,3) \notin R$.

(iv) R não é anti-simétrica porque $2R3$ e $3R2$, mas $2 \neq 3$.

(*c*) Para cada par $(a,b) \in R$, ache todos $(b, c) \in R$. Como $(a, c) \in R^2$,

$$R^2 = \{(1,1), (2,2), (2,3), (3,2), (3,3), (4,2), (4,3), (4,4)\}.$$

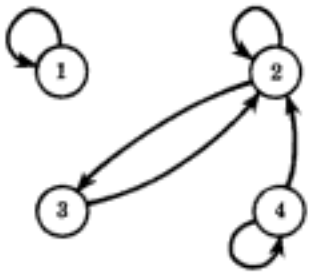


Fig. 2-10

2.14 Dê exemplos de relações R em $A = \{1, 2, 3\}$ que têm a propriedade requerida.

(*a*) R é simétrica e anti-simétrica.

(*b*) R não é nem simétrica nem anti-simétrica.

(*c*) R é transitiva, mas $R \cup R^{-1}$ não é transitiva.

Existem diversos exemplos possíveis para cada resposta. Segue um conjunto possível de exemplos:

(*a*) $R = \{(1, 1), (2, 2)\}$.

(*b*) $R = \{(1, 2), (2, 1), (2, 3)\}$.

(*c*) $R = \{(1, 2)\}$.

2.15 Suponha que C é uma coleção de relações S em um conjunto A, e seja T a interseção das relações S, isto é, $T = \cap\{S: S \in C\}$. Prove:

(*a*) Se toda S é simétrica, então T é simétrica.

(*b*) Se toda S é transitiva, então T é transitiva.

(*a*) Suponha $(a, b) \in T$. Então $(a, b) \in S$ para todo S. Como S é simétrica, $(b, a) \in S$ para todo S. Portanto, $(b, a) \in T$, e T é simétrica.

(*b*) Suponha que (a, b) e (b, c) pertencem a T. Então, (a, b) e (b, c) pertencem a S para todo S. Como cada S é transitiva, (a, c) pertence a S para todo S. Portanto, $(a, c) \in T$ e T é transitiva.

2.16 Seja R uma relação em um conjunto A, e seja P uma propriedade de relações, tal como simetria e transitividade. Então, P é chamada de R-fechável[†] se P satisfaz as duas condições seguintes:

(1) Existe uma P-relação S contendo R.

(2) A interseção de P-relações é uma P-relação.

(*a*) Mostre que simetria e transitividade são R-fecháveis para qualquer relação R.

(*b*) Suponha que P seja R-fechável. Então $P(R)$, o P-fecho de R, é a interseção de todas as P-relações S contendo R, isto é,

$$P(R) = \cap\{S: S \text{ é uma } P\text{-relação e } R \subseteq S\}.$$

(*a*) A relação universal $A \times A$ é simétrica e transitiva, e $A \times A$ contém qualquer relação R em A. Portanto, (1) é satisfeito. Pelo Problema 2-15, simetria e transitividade satisfazem (2). Portanto, simetria e transitividade são R-fecháveis para qualquer relação R.

[†] N. de T. No original, *R-closable*.

(*b*) Seja $T = \cap(S: S$ é uma P-relação e $R \subseteq S)$. Como P é R-fechável, T é não vazia por (1) e T é uma P-relação por (2). Como cada relação S contém R, a interseção T contém R. Portanto T é uma P-relação contendo R. Por definição, $P(R)$ é a menor P-relação contendo R; portanto, $P(R) \subseteq T$. Por outro lado, $P(R)$ é um dos conjuntos S definindo T, isto é, $P(R)$ é uma P-relação e $R \subseteq P(R)$. Por isso, $T \subseteq P(R)$. Coerentemente, $P(R) = T$.

2.17 Considere o conjunto $A = \{a, b, c\}$ e a relação R em A definida por

$$R = \{(a, a),\ (a, b),\ (b, c),\ (c, c)\}$$

Ache (*a*) reflexivo(R); (*b*) simétrico(R); e (*c*) transitivo(R).

(*a*) O fecho reflexivo em R é obtido pela adição de todos os pares diagonais $A \times A$ a R que ainda não estão em R. Portanto,

$$\text{reflexivo}(R) = R \cup \{(b, b)\} = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$$

(*b*) O fecho simétrico de R é obtido pela adição a R de todos os pares em R^{-1} que ainda não estão em R. Portanto,

$$\text{simétrico}(R) = R \cup \{(b, a), (c, b)\} = \{(a, a), (a, b), (b, a), (b, c), (c, b), (c, c)\}$$

(c) O fecho transitivo em R, como tem três elementos, é obtido pela união de R com $R^2 = R \circ R$ e $R^3 = R \circ R \circ R$. Note que

$$R^2 = R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$
$$R^3 = R \circ R \circ R = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Portanto,

$$\text{transitivo}(R) = R \cup R^2 \cup R^3 = \{(a, a), (a, b), (a, c), (b, c), (c, c)\}$$

Relações de Equivalência e Partições

2.18 Considere o conjunto $\mathbf{Z}$ dos inteiros e um inteiro $m > 1$. Dizemos que x é congruente a y módulo m, escrevendo

$$x \equiv y \pmod{m}$$

se $x - y$ é divisível por m. Mostre que isto define uma relação de equivalência em $\mathbf{Z}$.

Precisamos mostrar que a relação é reflexiva, simétrica e transitiva.

(i) Para cada x em $\mathbf{Z}$, temos $x \equiv x \pmod{m}$ porque $x - x = 0$ é divisível por m. Portanto, a relação é reflexiva.

(ii) Suponha $x \equiv y \pmod{m}$; logo, $x - y$ é divisível por m. Então $-(x - y) = y - x$ também é divisível por m; logo, $y \equiv x \pmod{m}$. Portanto, a relação é simétrica.

(iii) Agora suponha $x \equiv y \pmod{m}$ e $y \equiv z \pmod{m}$; logo, $x - y$ e $y - z$ são, cada um deles, divisíveis por m. Então a soma

$$(x - y) + (y - z) = x - z$$

também é divisível por m; portanto, $x \equiv z \pmod{m}$. Então, a relação é transitiva. Conseqüentemente, a relação de congruência módulo m é uma relação de equivalência.

2.19 Seja A um conjunto de inteiros não nulos e seja $\approx$ a relação em $A \times A$ definida por

$$(a, b) \approx (c, d) \qquad \text{sempre que} \qquad ad = bc$$

Mostre que $\approx$ é uma relação de equivalência.

Precisamos mostrar que $\approx$ é reflexiva, simétrica e transitiva.

(i) *Reflexividade*: temos $(a,b) \approx (a,b)$ já que $ab = ba$. Portanto, $\approx$ é reflexiva.

(ii) *Simetria:* suponha $(a,b) \approx (c,d)$. Então $ad = bc$. Por conseguinte, $cb = da$ e, portanto, $(a,b) \approx (c,d)$. Assim, $\approx$ é simétrica.

(iii) *Transitividade*: suponha $(a,b) \approx (c,d)$ e $(c,d) \approx (e, f)$. Então, $ab = bc$ e $cf = de$. A multiplicação dos termos correspondentes da equação leva a $(ad)(cf) = (bc)(de)$. Cancelando $c \neq 0$ e $d \neq 0$ dos dois lados da equação, obtém-se $af = be$, e portanto $(a,b) \approx (e, f)$. Logo, $\approx$ é transitiva. Conseqüentemente, $\approx$ é uma relação de equivalência.

2.20 Seja R a seguinte relação de equivalência no conjunto $A = \{1, 2, 3, 4, 5, 6\}$:

$$R = \{(1,1), (1,5), (2,2), (2,3), (2,6), (3,2), (3,3), (3,6), (4,4), (5,1), (5,5), (6,2), (6,3), (6,6)\}.$$

Ache a partição de A *induzida por* R, i.e., ache as classes de equivalência de R.

Os elementos relacionados a 1 são 1 e 5; portanto,

$$[1] = \{1, 5\}.$$

Selecionamos um elemento que não pertence a [1], por exemplo, 2. Os elementos relacionados a 2 são 2, 3 e 6; portanto,

$$[2] = \{2, 3, 6\}.$$

O único elemento que não pertence a [1] ou [2] é 4. O único elemento relacionado a 4 é 4. Logo,

$$[4] = \{4\}.$$

Conseqüentemente,

$$[\{1, 5\}, \{2, 3, 6\}, \{4\}]$$

é a partição de A induzida por R.

2.21 Prove o Teorema 2.6: seja R uma relação de equivalência em um conjunto A. O quociente A/R é uma partição de A.

(i) $a \in [a]$, para todo $a \in A$.

(ii) $[a] = [b]$ se e somente se $(a, b) \in R$.

(iii) Se $[a] \neq [b]$, então $[\ a\ ]$ e $[\ b\ ]$ são disjuntos.

Demonstração de (i): como R é reflexiva, $(a, a) \in R$ para todo $a \in A$ e, portanto, $a \in [a]$.

Demonstração de (ii): suponha $(a,b) \in R$. Queremos mostrar que $[a] = [b]$. Seja $x \in [b]$; então, $(b, x) \in R$. Mas, por hipótese, $(a, b) \in R$ e, portanto, por transitividade, $(a, x) \in R$. Conseqüentemente, $x \in A$. Portanto, $[b] \subseteq [a]$. Para mostrar $[a] \subseteq [b]$, observamos que $(a, b) \in R$, implica, por simetria, que $(b, a) \in R$. Então, por um argumento similar que obtemos $[a] \subseteq [b]$. Conseqüentemente $[a] = [b]$.

Por outro lado, se $[a]=[b]$, então, por (i), $b \in [b] = [a]$; portanto, $(a, b) \in R$.

Demonstração de (iii): provamos, equivalentemente, a contrapositiva da afirmação:

$$\text{Se } [a] \cap [b] \neq \varnothing, \text{ então } \quad [a] = [b].$$

Se $[a] \cap [b] \neq \varnothing$, então existe um elemento $x \in A$ com $x \in [a] \cap [b]$. Portanto, $(a, x) \in R$ e $(b, x) \in R$. Por simetria, $(x, b) \in R$ e, por transitividade, $(a, b) \in R$. Conseqüentemente por (ii), $[a] = [b]$.

2.22 Considere o conjunto de palavras $W = \{$saúde, luva, sal, pato, peso, som$\}$. Ache W/R onde R é a relação de equivalência em W definida por (*a*) "tem o mesmo número de letras que" ou (*b*) "começa com a mesma letra que".

(*a*) As palavras com o mesmo número de letras pertencem à mesma célula; logo,

$$W/R = [\{\text{saúde}\}, \{\text{luva, pato, peso}\}, \{\text{sal, som}\}].$$

(*b*) As palavras que começam com a mesma letra pertencem à mesma célula; logo,

$$W/R = [\{\text{saúde, sal, som}\}, \{\text{luva}\}, \{\text{pato, peso}\}].$$

Ordenação Parcial

2.23 Seja ℓ uma coleção qualquer de conjuntos. A relação $\subseteq$ de inclusão de conjuntos define uma ordem parcial em ℓ?

Sim, já que a inclusão de conjuntos é reflexiva, anti-simétrica e transitiva. Isto é, para quaisquer conjuntos, A, B, C em ℓ, temos: (i) $A \subseteq A$; (ii) se $A \subseteq B$ e $B \subseteq A$, então $A = B$; (iii) se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

2.24 Considere o conjunto $\mathbf{Z}$ dos inteiros. Defina aRb se $b = a^r$ para algum inteiro positivo r. Mostre que R é uma relação de ordem parcial em $\mathbf{Z}$, isto é, mostre que R é (a) reflexiva; (b) anti-simétrica e (c) transitiva.

(*a*) R é reflexiva já que $a = a^1$.

(*b*) Suponha que $a\ R\ b$ e $b\ R\ a$, vale dizer $b=a^r$ e $a=b^s$. Então $a=(a^r)^s$. Existem três possibilidades: (i) $rs = 1$, (ii) $a = 1$ e (iii) $a = -1$. Se $rs = 1$, então $r = 1$ e $s = 1$ e, portanto, $a = b$. Se $a = 1$, então $b=1^r=1=a$ e, de modo similar, se $b = 1$, então $a = 1$. Finalmente, se $a = -1$, então $b = -1$ (já que $b \neq 1$) e $a = b$. Nos três casos, $a = b$. Portanto R é anti-simétrica.

(*c*) Suponha que $a\ R\ b$ e $b\ R\ c$ ocorrem, vale dizer, $b=a^r$ e $c=b^s$. Então, $c=(a^r)^s=a^{rs}$ e, por isso, $a\ R\ c$. Portanto, R é transitiva.

Concluímos que R é uma ordem parcial em **Z**.

Problemas Complementares

Relações

2.25 Seja W = {Marco, Érico, Paulo} e seja V= {Érico, Davi}. Ache (*a*) $W \times V$; (*b*) $V \times W$; (*c*) $V \times V$.

2.26 Sejam $S = \{a, b, c\}$, $T = \{b, c, d\}$ e $W = \{a, d\}$. Construa os três diagramas de $S \times T \times W$ e então ache $S \times T \times W$.

2.27 Ache x e y se (*a*) $(x + 2, 4) = (5, 2x + y)$; (*b*) $(y - 2, 2x + 1) = (x - 1, y + 2)$.

2.28 Prove que (*a*) $A \times (B \cap C) = (A \times B) \cap (A \times C)$; (*b*) $A \times (B \cup C) = (A \times B) \cup (A \times B)$.

2.29 Seja R a seguinte relação em $A = \{1, 2, 3, 4\}$:

$$R = \{(1,3), (1,4), (3,2), (3,3), (3,4)\}$$

(*a*) Ache a matriz M_R de R.
(*b*) Ache o domínio e a imagem de R.
(*c*) Ache R^{-1}.
(*d*) Desenhe o grafo orientado de R.
(*e*) Ache a relação composta $R \circ R$.

2.30 Sejam R e S as seguintes relações em $B = \{a, b, c, d\}$:

$$R = \{(a,a), (a,c), (c,b), (c,d), (d,b)\} \quad \text{e} \quad S = \{(b,a), (c,c), (c,d), (d,a)\}$$

Ache as seguintes relações compostas: (*a*) $R \circ S$; (*b*) $S \circ R$; (*c*) $R \circ R$; (*d*) $S \circ S$.

2.31 Seja R a relação nos inteiros positivos **N** definida pela equação $x + 3y = 12$; isto é,

$$R = \{(x, y): x + 3y = 12\}$$

(*a*) Escreva R como um conjunto de pares ordenados.
(*b*) Ache (i) o domínio de R, (ii) a imagem de R e (iii) R^{-1}.
(*c*) Ache a relação composta $R \circ R$.

Propriedades de Relações

2.32 Cada uma das frases seguintes define uma relação nos inteiros positivos **N**:

(1) "x é maior do que y".
(2) "xy é o quadrado de um inteiro".
(3) $x + y = 10$
(4) $x + 4y = 10$

Determine quais relações são (*a*) reflexiva; (*b*) simétrica, (*c*) anti-simétrica, (*d*) transitiva.

2.33 Sejam R e S relações em um conjunto A. Assumindo que A tem pelo menos três elementos, verifique se cada uma das afirmações seguintes é verdadeira ou falsa. Se falsa, dê um contra-exemplo no conjunto $A = \{1, 2, 3\}$.

(*a*) Se R e S são simétricas, então $R \cap S$ é simétrica.

(*b*) Se R e S são simétricas, então $R \cup S$ é simétrica.

(*c*) Se R e S são reflexivas, então $R \cap S$ é reflexiva

(*d*) Se R e S são reflexivas, então $R \cup S$ é reflexiva.

(*e*) Se R e S são transitivas, então $R \cup S$ é transitiva.

(*f*) Se R e S são anti-simétricas, então $R \cup S$ é anti-simétrica.

(*g*) Se R é anti-simétrica, então R^{-1} é anti-simétrica.

(*h*) Se R é reflexiva, então $R \cap R^{-1}$ é não vazia.

(*i*) Se R é simétrica, então $R \cap R^{-1}$ é não vazia.

2.34 Suponha que R e S sejam relações em um conjunto A, e R seja anti-simétrica. Prove que $R \cap S$ é anti-simétrica.

Relações de Equivalência

2.35 Prove que, se R é uma relação de equivalência em um conjunto A, então R^{-1} também é uma relação de equivalência em A.

2.36 Seja $S = \{1, 2, 3, \ldots, 19, 20\}$. Seja R a relação de equivalência em S definida por $x \equiv y \pmod 5$, isto é, $x - y$ é divisível por 5. Ache a partição de S induzida por R, i.e., o conjunto quociente S/R.

2.37 Seja $A = \{1, 2, 3, \ldots, 9\}$ e seja $\sim$ uma relação em $A \times A$ definida por

$$(a, b) \sim (c, d) \qquad \text{se} \qquad a + d = b + c.$$

(*a*) Prove que $\sim$ é uma relação de equivalência. (*b*) Ache $[(2, 5)]$, i.e., a classe de equivalência de $(2, 5)$.

Respostas dos Problemas Complementares

2.25 (*a*) $W \times V = \{(\text{Marco, Érico}), (\text{Marco, Davi}), (\text{Érico, Érico}), (\text{Érico, Davi}), (\text{Paulo, Érico}), (\text{Paulo, Davi})\}$.
(*b*) $V \times W = \{(\text{Érico, Marco}), (\text{Davi, Marco}), (\text{Érico, Érico}), (\text{Davi, Érico}), (\text{Érico, Paulo}), (\text{Davi, Paulo})\}$.
(*c*) $V \times V = \{(\text{Érico, Érico}), (\text{Érico, Davi}), (\text{Davi, Érico}), (\text{Davi, Davi})\}$.

2.26 Os três diagramas de $S \times T \times W$ são exibidos na Figura 2-11. O conjunto $S \times T \times W$ é igual a

$$\{(a, b, a), (a, b, d), (a, c, a), (a, c, d), (a, d, a), (a, d, d),$$
$$(b, b, a), (b, b, d), (b, c, a), (b, c, d), (b, d, a), (b, d, d),$$
$$(c, b, a), (c, b, d), (c, c, a), (c, c, d), (c, d, a), (c, d, d)\}$$

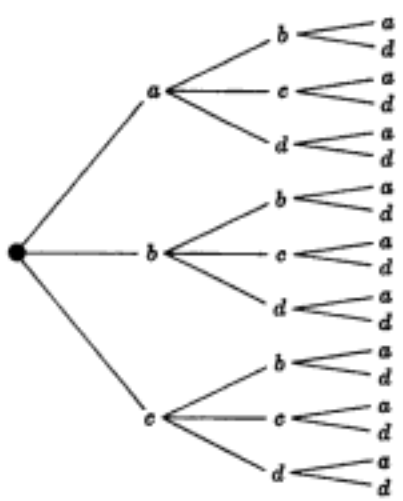


Fig. 2-11

2.27 (*a*) $x = 3; y = -2$; (*b*) $x = 2, y = 3$.

2.29 (*a*) $M_R = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

(*b*) Domínio $= \{1, 3\}$, imagem $= \{2, 3, 4\}$.
(*c*) $R^{-1} = \{(3, 1), (4, 1), (2, 3), (3, 3), (4, 3)\}$.
(*d*) Veja a Fig. 2-12.
(*e*) $R \circ R = \{(1, 2), (1, 3), (1, 4), (3, 2), (3, 3), (3, 4)\}$.

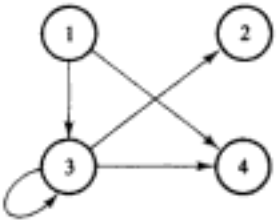


Fig. 2-12

2.30 (*a*) $R \circ S = \{(a, c), (a, d), (c, a), (d, a)\}$.
(*b*) $S \circ R = \{(b, a), (b, c), (c, b), (c, d), (d, a), (d, c)\}$.
(*c*) $R \circ R = \{(a, a), (a, b), (a, c), (a, d), (c, b)\}$.
(*d*) $S \circ S = \{(c, c), (c, a), (c, d)\}$.

2.31 (*a*) $\{(9, 1), (6, 2), (3, 3)\}$
(*b*) (i) $\{9, 6, 3\}$, (ii) $\{1, 2, 3\}$, (iii) $\{(1, 9), (2, 6), (3, 3)\}$
(*c*) $\{(3, 3)\}$

2.32 (*a*) Nenhuma; (*b*) (2) e (3); (*c*) (1) e (4); (*d*) todas, exceto (3).

2.33 Todas são verdadeiras exceto (*e*) $R = \{(1, 2)\}$, $S = \{(2, 3)\}$ e (*f*) $R = \{(1, 2)\}$, $S = \{(2, 1)\}$.

2.36 $[\{1, 6, 11, 16\}, \{2, 7, 12, 17\}, \{3, 8, 13, 18\}, \{4, 9, 14, 19\}, \{5, 10, 15, 20\}]$

2.37 (*b*) $\{(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 9)\}$

Capítulo 3

Funções e Algoritmos

3.1 INTRODUÇÃO

Um dos mais importantes conceitos em matemática é o de função. Os termos "mapeamento", "transformação" e muitos outros têm significados idênticos: a escolha de qual deles usar em cada situação é normalmente determinada pela tradição e pela experiência matemática de quem o está utilizando.

A noção de algoritmo está relacionada com a de função. A notação de apresentação de um algoritmo e a discussão sobre sua complexidade também são cobertas neste capítulo.

3.2 FUNÇÕES

Suponha que, a cada elemento de um conjunto A, associemos um único elemento de um conjunto B. A coleção destas associações é dita uma *função* de A em B. O conjunto A é dito o *domínio* da função, e o conjunto B é chamado de *contradomínio*.

Funções são normalmente denotadas por símbolos. Por exemplo, denote por f uma função de A em B. Então escrevemos

$$f: A \to B,$$

que se lê: "f é uma função de A em B", ou "f leva (ou mapeia) A em B". Se $a \in A$, então $f(a)$ (lê-se "f de a") denota o único elemento de B que f associa a a; ele é chamado a *imagem* de a por f, ou o *valor* de f em a. O conjunto de todos os valores da imagem é dito *imagem* de f. A imagem de $f: A \to B$ é denotada por $\text{Ran}(f)$, $\text{Im}(f)$ ou $f(A)$.

Freqüentemente uma função pode ser expressa por uma fórmula matemática. Por exemplo, considere a função que leva cada número real ao seu quadrado. Podemos descrever esta função escrevendo

$$f(x) = x^2 \qquad \text{ou} \qquad x \mapsto x^2 \qquad \text{ou} \qquad y = x^2$$

Na primeira notação, x é dito a *variável*, e a letra f denota a função. Na segunda notação, a seta $\mapsto$ é lida "vai em". Na última notação, x é dita a *variável independente*, e y é dita a *variável dependente*, já que o valor de y dependerá do valor de x.

Observação: Sempre que uma função é descrita por uma fórmula em termos de uma variável x, assumimos, a menos de especificação em contrário, que o domínio da função é $\mathbf{R}$ (ou o maior subconjunto de $\mathbf{R}$ para o qual a fórmula faz sentido), e o contradomínio é $\mathbf{R}$.

Exemplo 3.1

(*a*) Considere a função $f(x) = x^3$ i.e., *f* associa a cada número real seu cubo. Então a imagem de 2 é 8, e podemos escrever $f(2) = 8$.

(*b*) Suponha que *f* associa a cada país do mundo a sua capital. Aqui, o domínio de *f* é o conjunto de países do mundo; o contradomínio é a lista de cidades do mundo. A imagem de França é Paris; ou, em outras palavras, *f*(França) = Paris.

(*c*) A Figura 3-1 define uma função *f* de $A = \{a, b, c, d\}$ em $B = \{r, s, t, u\}$ de maneira clara. Aqui,

$$f(a) = s, \qquad f(b) = u, \qquad f(c) = r, \qquad f(d) = s$$

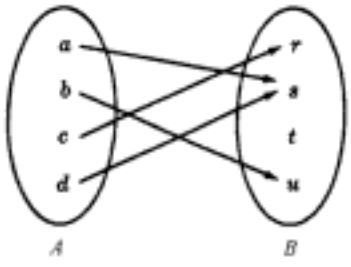


Fig. 3-1

A imagem de *f* é o conjunto de valores na imagem, $\{r, s, u\}$. Note que *r* não pertence à imagem de *f* porque *t* não é imagem de nenhum elemento por *f*.

(*d*) Seja *A* um conjunto qualquer. A função de *A* em *A* que associa cada elemento a si mesmo é dita *função identidade* em *A*, e é usualmente denotada por 1_A, ou simplesmente 1. Em outras palavras,

$$1_A(a) = a$$

para todo elemento *a* em *A*.

(*e*) Suponha que *S* seja um subconjunto de *A*, isto é, suponha $S \subseteq A$. A *inclusão*, ou *imersão*, de *S* em *A*, denotada por $i\colon S \hookrightarrow A$, é a função definida por

$$i(x) = x$$

para todo $x \in S$; e a *restrição* a *S* de qualquer função $f\colon A \to B$, denotada por $f|_S$, é a função de *S* para *B* definida por

$$f|_A(x) = f(x)$$

para todo $x \in S$.

Funções como Relações

As funções podem ser consideradas sob um outro ponto de vista. Primeiramente, toda função $f\colon A \to B$ origina uma relação de *A* para *B* chamada de *gráfico de f* e definida por

$$\text{Gráfico de } f = \{(a, b)\colon a \in A, b = f(a)\}$$

Duas funções $f\colon A \to B$ e $g\colon A \to B$ são ditas iguais, $f = g$, se $f(a) = g(a)$ para todo $a \in A$; isto é, se elas têm o mesmo gráfico. Conseqüentemente, não distinguimos uma função do seu gráfico. A relação descrita pelo gráfico tem a propriedade de cada *a* em *A* pertence a um único par ordenado (a, b) na relação. Por outro lado, qualquer relação *f* de *A* para *B* que tem essa propriedade origina uma função $f\colon A \to B$, onde $f(a) = b$ para cada (a, b) em *f*.Conseqüentemente, pode-se definir funções como a seguir:

Definição: Uma função $f\colon A \to B$ é uma relação de *A* para *B* (i.e., um subconjunto de $A \times B$) tal que cada $a \in A$ pertence a um único par ordenado (a, b) em *f*.

Embora não façamos distinção entre uma função e seu gráfico, usaremos a terminologia "gráfico de *f*" quando aludirmos a *f* como um conjunto de pares ordenados. Além disso, como o gráfico de *f* é uma relação, podemos esboçar seu desenho como foi feito para relações em geral, e esse desenho é, às vezes, chamado de gráfico de *f*. Além disso, a condição que define uma função de que $a \in A$ pertence a um único (a, b) em *f* é equivalente à condição geométrica de que cada reta vertical intercepta o gráfico de *f* em exatamente um ponto.

Exemplo 3.2

(*a*) Seja $f\colon A \to B$ a função definida no Exemplo 3.1(*c*). Então, o gráfico de *f* é o seguinte conjunto de pares ordenados:

$$\{(a, s), (b, u), (c, r), (d, s)\}$$

(*b*) Considere as seguintes relações no conjunto $A = \{1, 2, 3\}$:

$$f = \{(1,3), (2,3), (3,1)$$
$$g = \{(1,2), (3,1)\}$$
$$h = \{(1,3), (2,1), (1,2), (3,1)\}$$

f é uma função de A em A, já que cada elemento de A aparece na primeira coordenada em exatamente um par ordenado em f; aqui, $f(1)=3$, $f(2) = 3$ e $f(3) = 1$. g não é uma função de A em A, já que $2 \in A$ não é a primeira coordenada de nenhum par em g e, portanto, g não associa nenhuma imagem a 2. Também h não é uma função de A em A, já que $1 \in A$ aparece como primeira coordenada de dois pares ordenados distintos em h, (1, 3) e (1, 2). Para que h seja uma função, os elementos tanto 3 quanto 2 não podem estar associados ao elemento $1 \in A$.

(*c*) Por uma função polinomial real, entendemos uma função f: $\mathbf{R} \to \mathbf{R}$ da forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

onde cada a_i é um número real. Como $\mathbf{R}$ é um conjunto infinito, seria impossível plotar cada ponto do gráfico. Entretanto, o gráfico de uma tal função pode ser aproximado plotando inicialmente alguns pontos e depois traçando uma curva suave que contenha tais pontos. Os pontos são normalmente obtidos de uma tabela onde vários valores são atribuídos a x e os valores correspondentes de $f(x)$ são computados. A Figura 3-2 ilustra esta técnica usando a função $f(x) = x^2 - 2x - 3$.

x	$f(x)$
−2	5
−1	0
0	−3
1	−4
2	−3
3	0
4	5

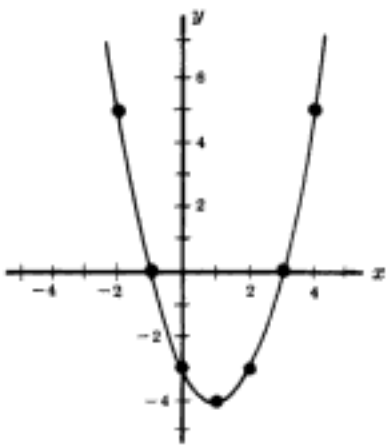


Gráfico de $f(x) = x^2 - 2x - 3$

Fig. 3-2

Composição de Funções

Considere as funções f: $A \to B$ e g : $B \to C$, isto é, o contradomínio de f é o domínio de g. Então, podemos definir uma nova função de A para C, denominada a *composição* de f e g e denotada por $g \circ f$, como se segue:

$$(g \circ f)(a) \equiv g(f(a))$$

Isto é, achamos a imagem de a por f e então achamos a imagem de $f(a)$ por g. Essa definição não é nova. Se olharmos f e g como relações, esta função é a mesma que a composição de f e g como relações (veja a Seção 2.6), exceto pelo fato de aqui usarmos a notação funcional $g \circ f$ para a composição de f e g em vez da notação $g \circ f$ que foi usada para relações.

Considere uma função qualquer f: $A \to B$. Então,

$$f \circ 1_A = f \quad \text{e} \quad 1_B \circ f = f$$

onde 1_A e 1_B são as funções identidade em A e B, respectivamente.

3.3 INJETIVIDADE, SOBREJETIVIDADE E FUNÇÕES INVERSÍVEIS

Uma função $f: A \to B$ é dita *injetora*[†] (denotada por 1-1) se elementos diferentes do domínio A têm imagens distintas. Outra maneira de dizer a mesma coisa é afirmar que f é *injetora* se $f(a) = f(a')$ implica $a = a'$.

Uma função $f: A \to B$ é dita uma função *sobrejetora*[††] se cada elemento de B é a imagem de algum elemento de A. Em outras palavras, $f: A \to B$ é *sobrejetora* se a imagem de f é todo o contradomínio, i.e., $f(A) = B$. Neste caso dizemos que f é uma função de A *sobre* B ou que f mapeia A *sobre* B.

Uma função $f: A \to B$ é *inversível* se a relação inversa é uma função de B para A. Em geral, a relação inversa f^{-1} pode não ser uma função. O teorema seguinte indica um critério simples que diz em que caso isso ocorre.

Teorema 3-1: uma função $f: A \to B$ é inversível se e somente se f é injetora e sobrejetora.

Se $f: A \to B$ é injetora e sobrejetora, f é dita uma *correspondência um-a-um* entre A e B. Essa terminologia decorre do fato de que, a cada elemento de A, corresponderá um único elemento de B e vice-versa.

Alguns textos usam o termo *injetiva* para funções *one-to-one*, *sobrejetiva* para uma função *onto* e *bijetiva* para uma correspondência um-a-um[†††].

Exemplo 3.3 Considere as funções $f_1: A \to B$, $f_2: B \to C$, $f_3: C \to D$ e $f_4: D \to E$ definidas pelo diagrama da Figura 3-3. Agora, f_1 é injetora, já que nenhum elemento de B é a imagem de mais de um elemento de A. Analogamente, f_2 é injetora. Entretanto, nem f_3 nem f_4 são injetoras, já que $f_3(r) = f_3(u)$ e $f_4(v) = f_4(w)$.

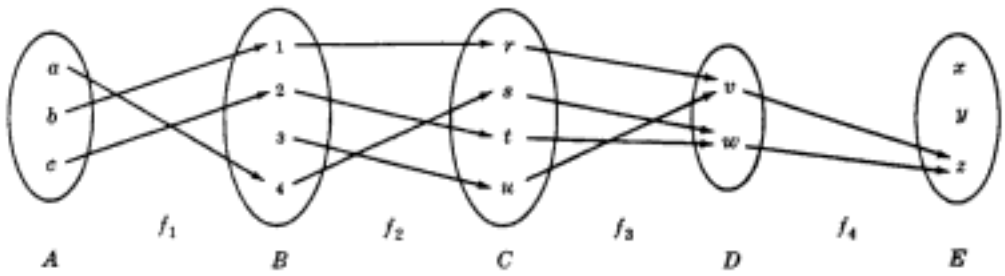


Fig. 3-3

No que diz respeito à sobrejetividade, f_2 e f_3 são funções sobrejetoras, já que todo elemento de C é a imagem por f_2 de algum elemento de B, e todo elemento de D é a imagem por f_3 de algum elemento de C, i. e., $f_2(B) = C$ e $f_3(C) = D$. Por outro lado, f_1 não é sobrejetora já que $3 \in B$ não é a imagem por f_1 de nenhum elemento de A, e f_4 não é sobrejetora já que $x \in E$ não é a imagem por f_4 de nenhum elemento de D.

Portanto, f_1 é injetora mas não sobrejetora, f_3 é sobrejetora mas não injetora e f_4 não é nem injetora nem sobrejetora. Entretanto, f_2 é injetora e sobrejetora, i.e., é uma correspondência um-a-um entre A e B. Portanto, f_2 é inversível e f_2^{-1} é uma função de C para B.

Caracterização Geométrica de Funções Injetoras e Sobrejetoras

Como as funções podem ser identificadas com seus gráficos, e como gráficos podem ser plotados, poderíamos imaginar se os conceitos de injetividade e sobrejetividade têm significado geométrico. Mostramos que a resposta é sim.

Dizer que uma função $f: A \to B$ é injetora significa afirmar que não existem dois pares distintos da forma (a_1, b) e (a_2, b) no gráfico de f; portanto, cada reta horizontal pode interceptar o gráfico de f em, no máximo, um ponto. Por outro lado, dizer que f é uma função sobrejetora significa afirmar que, para todo $b \in B$, existe pelo menos um $a \in A$ tal que (a,b) pertence ao gráfico de f; portanto, cada linha horizontal deve interceptar o gráfico de f pelo menos uma vez. Conseqüentemente, se f é injetora e sobrejetora, i.e. inversível, então cada linha horizontal intercepta o gráfico de f em exatamente um ponto.

[†] N. de T. No original, *one-to-one*, termo cuja tradução literal é de uso raro em português. Entretanto, a notação (1-1) (por vezes também indicando bijetividade) é encontrada com freqüência.

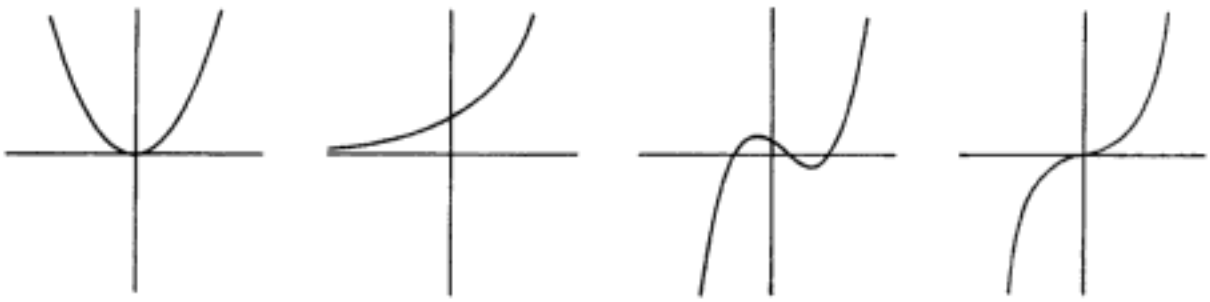
[††] N. de T. No original *onto*, termo cuja tradução literal (sobre) é de uso raro em português neste caso.

[†††] N. de T. Esta é, de fato, a nomenclatura comumente usada em português.

Exemplo 3.4 Considere as seguintes quatro funções de $\mathbf{R}$ em $\mathbf{R}$:

$$f_1(x) = x^2, \qquad f_2(x) = 2^x, \qquad f_3(x) = x^3 - 2x^2 - 5x + 6, \qquad f_4(x) = x^3$$

Os gráficos dessas funções aparecem na Figura 3-4. Observe que existem retas horizontais que interceptam o gráfico de f_1 duas vezes e retas verticais que não interceptam o gráfico de f_1; portanto, f_1 não é nem injetora nem sobrejetora. Analogamente, f_2 é injetora mas não sobrejetora, f_3 é sobrejetora mas não injetora e f_4 é injetora e sobrejetora. A inversa de f_4 é a função raiz cúbica, i.e., $f_4^{-1}(x) = \sqrt[3]{x}$.



$f_1(x) = x^2$ $\quad$ $f_2(x) = 2^x$ $\quad$ $f_3(x) = x^3 - 2x^2 - 5x + 6$ $\quad$ $f_4(x) = x^3$

Fig. 3-4

3.4 FUNÇÕES MATEMÁTICAS, FUNÇÕES EXPONENCIAL E LOGARITMO

Esta seção apresenta várias funções matemáticas que aparecem com freqüência na análise de algoritmos e na ciência da computação em geral, juntamente com suas notações. Também discutimos as funções exponencial e logaritmo e a relação entre elas.

Funções *Floor* e *Ceiling*

Seja x um número real qualquer. Então x está entre dois inteiros conhecidos como *floor* e *ceiling*[†] de x. Especificamente,

$\lfloor x \rfloor$, dito *floor* de x, denota o maior inteiro que não excede x.
$\lceil x \rceil$, dito *ceiling* de x, denota o menor inteiro que não é menor do que x.

Se x é um inteiro, então $\lfloor x \rfloor = \lceil x \rceil$; caso contrário, $\lfloor x \rfloor + 1 = \lceil x \rceil$. Por exemplo,

$$\lfloor 3{,}14 \rfloor = 3, \quad \lfloor \sqrt{5} \rfloor = 2, \quad \lfloor -8{,}5 \rfloor = -9, \quad \lfloor 7 \rfloor = 7, \quad \lfloor -4 \rfloor = -4$$
$$\lceil 3{,}14 \rceil = 4, \quad \lceil \sqrt{5} \rceil = 3, \quad \lceil -8{,}5 \rceil = -8, \quad \lceil 7 \rceil = 7, \quad \lceil -4 \rceil = -4$$

Funções Valor Inteiro e Valor Absoluto

Seja x um número real qualquer. O *valor inteiro* de x, escrito $\text{INT}(x)$, converte x em um inteiro deletando (truncando) a parte fracionária do número. Portanto,

$$\text{INT}(3{,}14) = 3, \qquad \text{INT}(\sqrt{5}) = 2, \qquad \text{INT}(-8{,}5) = -8, \qquad \text{INT}(7) = 7$$

Observe que $\text{INT}(x) = \lfloor x \rfloor$ ou $\text{INT}(x) = \lceil x \rceil$, dependendo de x ser positivo ou negativo.

O *valor absoluto* de um número real x, denotado por $\text{ABS}(x)$ ou $|x|$, é definido como sendo o maior dos valores entre x e $-x$. Portanto, $\text{ABS}(0) = 0$ e, para $x \neq 0$, $\text{ABS}(x) = x$, ou $\text{ABS}(x) = -x$, dependendo de x ser positivo ou negativo. Portanto,

$$|-15| = 15, \qquad |7| = 7, \qquad |-3{,}33| = 3{,}33, \qquad |4{,}44| = 4{,}44, \qquad |-0{,}075| = 0{,}075$$

Notamos que $|x| = |-x|$ e, para $x \neq 0$, $|x|$ é positivo.

[†] N. de T. Mantivemos a nomenclatura original em inglês devido à ausência de termo análogo de uso corrente em textos técnicos. Em português, estas funções são normalmente referenciadas como, respectivamente, "menor inteiro maior ou igual a x" e "maior inteiro menor ou igual a x".

Função Resto e Aritmética Modular

Seja k um inteiro qualquer e seja M um inteiro positivo. Então,

$$k \pmod{M}$$

(lê-se k módulo M) denotará o resto inteiro da divisão de k por M. Mais exatamente, $k(\text{mod } M)$ é o único inteiro r tal que

$$k = Mq + r \qquad \text{onde} \qquad 0 \leq r < M$$

Quando k é positivo, simplesmente divida k por M para obter o resto r. Portanto,

$$25 \pmod{7} = 4, \qquad 25 \pmod{5} = 0, \qquad 35 \pmod{11} = 2, \qquad 3 \pmod{8} = 3$$

Se k é negativo, divida $|k|$ por M para obter o resto r'; portanto, $k(\text{mod } M) = M - r'$ quando $r' \neq 0$. Assim,

$$-26 \pmod{7} = 7 - 5 = 2, \qquad -371 \pmod{8} = 8 - 3 = 5, \qquad -39 \pmod{3} = 0$$

O termo "mod" é também usado para a relação de congruência, que é denotada e definida como a seguir:

$$a \equiv b \pmod{M} \quad \text{se e somente se} \quad M \text{ divide } b - a$$

M é dito o *modulus*[†], e $a \equiv b \pmod{M}$ é lido como "a é congruente a b módulo M". Os seguintes aspectos da relação de congruência são usados com freqüência:

$$0 \equiv M \pmod{M} \quad \text{e} \quad a \pm M \equiv a \pmod{M}$$

Aritmética módulo M se refere às operações aritméticas de adição, multiplicação e subtração em que o valor aritmético é substituído pelo seu valor equivalente no conjunto

$$\{0, 1, 2, \ldots, M - 1\}$$

ou no conjunto

$$\{1, 2, 3, \ldots, M\}$$

Por exemplo, na aritmética módulo 12, às vezes chamada de aritmética *clock*,

$$6 + 9 \equiv 3, \qquad 7 \times 5 \equiv 11, \qquad 1 - 5 \equiv 8, \qquad 2 + 10 \equiv 0 \equiv 12$$

(O uso de 0 ou M depende da aplicação.)

Funções Exponenciais

Relembre as seguintes definições para expoentes inteiros (onde m é um inteiro positivo):

$$a^m = a \cdot a \cdots a \,(m \text{ vezes}), \qquad a^0 = 1, \qquad a^{-m} = \frac{1}{a^m}$$

Expoentes são estendidos para incluir todos os números racionais definindo, para qualquer número racional m/n,

$$a^{m/n} = \sqrt[n]{a^m} = (\sqrt[n]{a})^m$$

Por exemplo,

$$2^4 = 16, \qquad 2^{-4} = \frac{1}{2^4} = \frac{1}{16}, \qquad 125^{2/3} = 5^2 = 25$$

Na verdade, expoentes são estendidos para incluir todos os números reais definindo, para qualquer número real x,

$$a^x = \lim_{r \to x} a^r, \text{ onde } r \text{ é um número racional.}$$

Conseqüentemente a função exponencial $f(x) = a^x$ é definida para todos os números reais.

[†] N. de T. Nomenclatura constante no original.

Funções Logarítmicas

Logaritmos são relacionados com expoentes como a seguir. Seja b um número positivo. O logaritmo de qualquer número positivo x na base b, denotado por

$$\log_b x$$

representa o expoente ao qual b precisa ser elevado para obter x. Isto é,

$$y = \log_b x \quad \text{e} \quad b^y = x$$

são afirmativas equivalentes. Conseqüentemente,

$$\log_2 8 = 3 \quad \text{já que} \quad 2^3 = 8; \qquad \log_{10} 100 = 2 \quad \text{já que} \quad 10^2 = 100$$
$$\log_2 64 = 6 \quad \text{já que} \quad 2^6 = 64; \qquad \log_{10} 0{,}001 = -3 \quad \text{já que} \quad 10^{-3} = 0{,}001$$

Ademais, para qualquer base b,

$$\log_b 1 = 0 \quad \text{já que} \quad b^0 = 1$$
$$\log_b b = 1 \quad \text{já que} \quad b^1 = b$$

O logaritmo de um número negativo e o logaritmo de 0 não são definidos.

Freqüentemente, logaritmos são expressados usando valores aproximados. Por exemplo, usando tabelas ou calculadoras, obtêm-se

$$\log_{10} 300 = 2{,}4771 \qquad \text{e} \qquad \log_e 40 = 3{,}6889$$

como respostas aproximadas (aqui, $e = 2{,}718281\ldots$).

Três classes de logaritmos têm importância especial: logaritmos na base 10, chamados *logaritmos decimais*[†]; logaritmo na base e, chamados de *logaritmos naturais*; e logaritmos na base 2, chamados *logaritmos binários*. Alguns textos utilizam

$$\ln x \quad \text{para} \quad \log_e x \qquad \text{e} \qquad \lg x \quad \text{ou} \quad \text{Log } x \quad \text{para} \quad \log_2 x$$

O termo $\log x$, em geral, significa $\log_{10} x$, mas também é usado para $\log_e x$ em textos de matemática avançada e para $\log_2 x$ em textos de ciência da computação.

Freqüentemente, vamos necessitar apenas do *floor* e do *ceiling* de um logaritmo binário. Isso pode ser obtido pela inspeção das potências de 2. Por exemplo,

$$\lfloor \log_2 100 \rfloor = 6 \quad \text{já que} \quad 2^6 = 64 \quad \text{e} \quad 2^7 = 128$$
$$\lceil \log_2 1000 \rceil = 9 \quad \text{já que} \quad 2^8 = 512 \quad \text{e} \quad 2^9 = 1024$$

e assim por diante.

Relação entre as Funções Exponencial e Logaritmo

A relação básica entre as funções exponencial e logaritmo

$$f(x) = b^x \qquad \text{e} \qquad g(x) = \log_b x$$

é que elas são a inversa uma da outra; logo, os gráficos dessas funções estão relacionados geometricamente. Esta relação está ilustrada na Figura 3-5, onde os gráficos da função exponencial $f(x) = 2^x$, da função logaritmo $g(x) = \log_2 x$ e da função linear $h(x) = x$ aparecem nos mesmos eixos coordenados. Como $f(x) = 2^x$ e $g(x) = \log_2 x$ são funções inversas uma da outra, elas são simétricas em relação ao gráfico da função linear $h(x) = x$, ou, em outras palavras, a reta $y = x$.

A Figura 3-5 também indica uma outra propriedade importante das funções exponencial e logaritmo. Especificamente, para qualquer número positivo c, temos

$$g(c) < h(c) < f(c)$$

[†] N. de T. No original *common logarithms*.

De fato, à medida que c cresce, a distância vertical $h(c) - g(c)$ e $f(c) - g(c)$ aumenta seu valor. Ademais, a função logaritmo $g(x)$ cresce muito lentamente quando comparada com a função linear $h(x)$, e a função exponencial $f(x)$ cresce muito rapidamente quando comparada com $h(x)$.

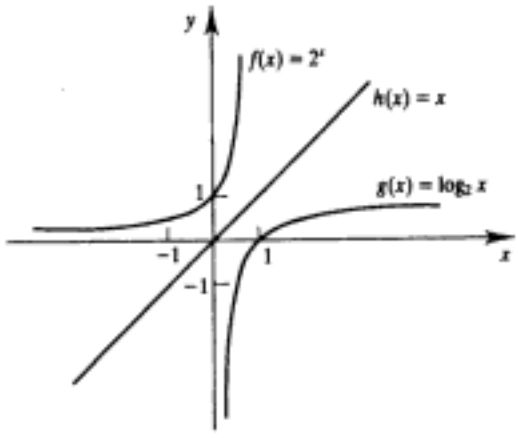


Fig. 3-5

3.5 SEQÜÊNCIAS, CLASSES INDEXADAS DE CONJUNTOS

Seqüências e classes indexadas de conjuntos são tipos especiais de funções com sua notação própria. Discutimos esses objetos nesta seção. Discutimos também aqui a notação de somatório.

Seqüências

Uma *seqüência* é uma função injetora do conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ dos inteiros positivos em um conjunto A. A notação a_n é usada para denotar a imagem do inteiro n. Portanto, uma seqüência é usualmente denotada por

$$a_1, a_2, a_3, \ldots \qquad \text{ou} \qquad \{a_n : n \in \mathbf{N}\} \qquad \text{ou} \quad \text{simplesmente} \qquad \{a_n\}$$

Às vezes o domínio da seqüência é o conjunto $\{0, 1, 2, \ldots\}$ dos inteiros não-negativos, no lugar de $\mathbf{N}$. Neste caso, dizemos que n começa em 0, e não em 1.

Uma *seqüência finita* sobre um conjunto A é uma função de $a\ \{1,2,\ldots, m\}$ em A e é usualmente denotada por

$$a_1, a_2, \ldots, a_m$$

Uma tal seqüência finita às vezes é denominada *lista* ou *m-upla*.

Exemplo 3.5

(*a*) As seqüências conhecidas

$$1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \ldots \qquad \text{e} \qquad 1, \tfrac{1}{2}, \tfrac{1}{4}, \tfrac{1}{8}, \ldots$$

podem ser formalmente definidas, respectivamente, por

$$a_n = 1/n \qquad \text{e} \qquad b_n = 2^{-n}$$

onde a primeira seqüência começa com $n = 1$ e a segunda começa com $n = 0$.

(*b*) A importante seqüência $1, -1, 1, -1, \ldots$ pode ser formalmente definida por

$$a_n = (-1)^{n+1} \qquad \text{ou equivalentemente por} \qquad b_n = (-1)^n$$

onde a primeira seqüência começa com $n = 1$ e a segunda seqüência começa com $n = 0$.

(*c*) (***Strings***) Suponha que um conjunto A é finito e que A é um conjunto de caracteres ou um alfabeto. Então, uma seqüência finita de elementos de A é dita um *string* ou uma *palavra*, e é normalmente escrita na forma $a_1 a_2 \ldots a_m$, isto é, sem parênteses. O número m de caracteres no *string* é dito o seu *comprimento*. Pode-se considerar o conjunto com zero caracteres como um *string*; ele é denominado *string vazio* ou *string nulo*. *Strings* sobre um alfabeto A e certas operações envolvendo *strings* serão discutidos no Capítulo 13.

Símbolos de Somatório, Somas

Introduzimos aqui o símbolo de somatório Σ (a letra grega sigma). Considere a seqüência $a_1, a_2, a_3, \ldots$ Então, as somas

$$a_1 + a_2 + \cdots + a_n \qquad \text{e} \qquad a_m + a_{m+1} + \cdots + a_n$$

serão denotadas, respectivamente, por

$$\sum_{j=1}^{n} a_j \qquad \text{e} \qquad \sum_{j=m}^{n} a_j$$

A letra j na expressão acima é denominada *índice mudo* ou *variável muda*[1]. Outras letras freqüentemente utilizadas como variáveis mudas são i, k, s e t.

Exemplo 3.6

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$$

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54$$

$$\sum_{j=1}^{n} j = 1 + 2 + \cdots + n$$

A última soma no Exemplo 3.6 aparece com freqüência. Seu valor é $n(n + 1)/2$. Isto é,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Portanto, por exemplo,

$$1 + 2 + \cdots + 50 = \frac{50(51)}{2} = 1.275$$

Classes Indexadas de Conjuntos

Seja I um conjunto qualquer não vazio e seja S uma coleção de conjuntos. Uma *função indexadora* de I para S é uma função f: $I \to S$. Para cada i em I, denotamos a imagem $f(i)$ por A_i. Assim, a função indexadora f é denotada por

$$\{A_i : i \in I\} \qquad \text{ou} \qquad \{A_i\}_{i \in I} \qquad \text{ou simplesmente} \qquad \{A_i\}$$

O conjunto I é dito o *conjunto indexador*, e os elementos de I são chamados *índices*. Se f é injetora e sobrejetora, dizemos que S é *indexada* por I.

Os conceitos de união e interseção de conjuntos são definidos para classes indexadas de conjuntos por

$$\cup_{i \in I} A_i = \{x : x \in A_i \text{ para algum } i \in I\} \qquad \text{e} \qquad \cap_{i \in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}$$

No caso em que I é um conjunto finito, essa é exatamente a definição dada previamente de união e interseção. Se I é $\mathbf{N}$, podemos denotar a união e a interseção por

$$A_1 \cup A_2 \cup \cdots \qquad \text{e} \qquad A_1 \cap A_2 \cap \cdots$$

respectivamente.

[1] N. de T. No original *dummy*.

Exemplo 3.7 Seja I o conjunto $\mathbf{Z}$ dos inteiros. Para cada inteiro n, associamos o seguinte subconjunto de $\mathbf{R}$:

$$A_n = \{x: x \leq n\}$$

Em outras palavras, A_n é o intervalo infinito $[-\infty, n]$. Para qualquer número real a, existem inteiros n_1 e n_2 tais que $n_1 < a < n_2$; logo, $a \in An_2$, mas $a \notin An_1$. Portanto,

$$a \in \cup_n A_n \qquad \text{mas} \qquad a \notin \cap_n A_n$$

Conseqüentemente,

$$\cup_n A_n = \mathbf{R} \qquad \text{mas} \qquad \cap_n A_n = \varnothing$$

3.6 FUNÇÕES DEFINIDAS RECURSIVAMENTE

Uma função é dita *recursivamente definida* se a definição da função se referir à própria função. Para que a definição não seja circular, precisa satisfazer as duas seguintes propriedades:

(1) Devem existir certos argumentos, chamados de *valores base*, nos quais a função não se referencie a ela mesma.

(2) Cada vez que a função se referir a si própria, o argumento da função precisa estar próximo a um valor base.

Uma função recursiva com essas duas propriedades é dita bem definida.

Os exemplos seguintes ajudarão a esclarecer essas noções.

Função Fatorial

O produto de um inteiro positivo de 1 até n, inclusive, é chamado "fatorial de n" e é normalmente denotado por $n!$. Isto é,

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-2)(n-1)n$$

Também é conveniente definir $0! = 1$, de modo que a função esteja definida para todo inteiro não negativo. Assim, temos

$$0! = 1, \qquad 1! = 1, \qquad 2! = 1 \cdot 2 = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24,$$

$$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120, \qquad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$$

e assim por diante. Observe que

$$5! = 5 \cdot 4! = 5 \cdot 24 = 120 \qquad \text{e} \qquad 6! = 6 \cdot 5! = 6 \cdot 120 = 720$$

Isto é verdade para todo inteiro positivo n; isto é,

$$n! = n \cdot (n-1)!$$

Por conseguinte, a função fatorial também pode ser definida como a seguir:

Definição de Função fatorial:

(1) Se $n = 0$, então $n! = 1$.

(2) Se $n > 0$, então $n! = n \cdot (n-1)!$

Observe que a definição acima de $n!$ é recursiva, já que se refere a si própria quando usa $(n-1)!$. Entretanto:

(1) O valor de $n!$ é dado explicitamente quando $n = 0$ (portanto, 0 é um valor base).

(2) O valor de $n!$ para n arbitrário é definido em termos de um valor menor do que n que está mais próximo do valor base 0.

Conseqüentemente, a definição não é circular, ou, em outras palavras, a função é bem definida.

Exemplo 3.8 Vamos calcular 4! usando as definições recursivas. Esse cálculo requer os nove passos seguintes:

(1) $4! = 4 \cdot 3!$
(2) $3! = 3 \cdot 2!$
(3) $2! = 2 \cdot 1!$
(4) $1! = 1 \cdot 0!$
(5) $0! = 1$
(6) $1! = 1 \cdot 1 = 1$
(7) $2! = 2 \cdot 1 = 2$
(8) $3! = 3 \cdot 2 = 6$
(9) $4! = 4 \cdot 6 = 24$

Isto é:

Passo 1 Define 4! em termos de 3!, e assim precisamos adiar a avaliação de 4! até que calculemos 3!. Esse adiamento está indicado na tabulação do passo seguinte.

Passo 2 Aqui 3! é definido em termos de 2!, e assim precisamos adiar a avaliação de 3! até que avaliemos 2!.

Passo 3 Define 2! em termos de 1!.

Passo 4 Define 1! em termos de 0!.

Passo 5 Este passo pode avaliar explicitamente 0!, já que 0 é o valor base da definição recursiva.

Passos 6 a 9 Retrocedemos o processo, usando 0! para achar 1!, usando 1! para achar 2!, usando 2! para achar 3!, e finalmente usando 3! para achar 4!. Este retrocesso é indicado pela reversão progressiva dos afastamentos na tabulação.

Observe que retrocedemos na ordem reversa das avaliações originalmente adiadas.

Números de nível

Seja P um procedimento[†] ou uma fórmula recursiva usada para avaliar $f(X)$, onde f é uma função recursiva e X é a entrada. Associamos um número de nível a cada execução de P como segue. A primeira execução de P é associada ao nível 1 e, a cada vez que P é executada devido a uma chamada recursiva, seu nível é uma unidade maior do que o nível da execução que fez a chamada. A profundidade de uma recursão na avaliação de $f(X)$ se refere ao maior número de nível de P durante a sua execução.

Considere, por exemplo, a avaliação de 4!, Exemplo 3.8, que usa a fórmula recursiva $n! = n(n-1)!$. O Passo 1 pertence ao nível 1, já que é a primeira vez que a fórmula é executada. Assim:

Passo 2 pertence ao nível 2; Passo 3, ao nível 3,...; Passo 5, ao nível 5.

Por outro lado, o Passo 6 pertence ao nível 4, já que é o resultado do retorno do nível 5. Em outras palavras, o Passo 6 e o Passo 4 pertencem ao mesmo nível de execução. Analogamente,

Passo 7 pertence ao nível 3; Passo 8, ao nível 2; e o Passo 9, ao nível 1.

Conseqüentemente, na avaliação de 4!, a profundidade da recursão é 5.

Seqüência de Fibonacci

A célebre seqüência de Fibonacci (normalmente denotada por $F_0, F_1, F_2, \ldots$) é:

$$0, \quad 1, \quad 1, \quad 2, \quad 3, \quad 5, \quad 8, \quad 13, \quad 21, \quad 34, \quad 55, \ldots$$

Isto é, $F_0 = 0$ e $F_1 = 1$ e cada termo, na sucessão, é a soma dos dois termos precedentes. Por exemplo, os dois termos seguintes da seqüência são

$$34 + 55 = 89 \quad \text{e} \quad 55 + 89 = 144$$

Uma definição formal desta função é dada por:

[†] N. de T. No original, *procedure*, também usado com freqüência na linguagem de ciência da computação no sentido de rotina computacional.

Definição de Seqüência de Fibonacci:

(1) Se $n = 0$ ou $n = 1$, então $F_n = n$
(2) Se $n > 1$, então $F_n = F_{n-2} + F_{n-1}$

Este é um outro exemplo de definição recursiva, já que a definição refere-se a si mesma quando usa F_{n-2} e F_{n-1}. Contudo,

(1) Os valores base são 0 e 1.
(2) O valor de F_n é definido em termos de valores menores do que n que estão mais próximos dos valores base.

Conseqüentemente, a função é bem definida.

Função de Ackermann

A função de Ackermann é uma função com dois argumentos, a cada um dos quais pode ser atribuído um inteiro não negativo, isto é, 0, 1, 2,... Esta função é definida como a seguir:

Definição de Função de Ackermann:

(*a*) Se $m = 0$, então $A(m, n) = n + 1$
(*b*) Se $m \neq 0$, mas $n = 0$, então $A(m, n) = A(m - 1, 1)$
(*c*) Se $m \neq 0$ e $n \neq 0$, então $A(m, n) = A(m - 1, A(m, n - 1))$

Mais uma vez, temos uma definição recursiva, já que a definição refere-se a si mesma nas partes (*b*) e (*c*). Observe que $A(m, n)$ é explicitamente dada apenas quando $m = 0$. Os pares usados no cálculo são

$$(0,0), \quad (0,1), \quad (0,2), \quad (0,3), \ldots, (0,n), \ldots$$

Embora não seja óbvio na definição, o valor de qualquer $A(m, n)$ pode ser expresso em termos do valor da função em um ou mais dos pares base.

O valor de $A(1, 3)$ é calculado no Problema 3.24. Mesmo este simples caso requer 15 passos. Em linhas gerais, a função de Ackermann é muito complexa para ser avaliada em qualquer exemplo que não seja trivial. Sua importância advém do seu uso na lógica matemática. A função é definida aqui principalmente para apresentar mais um exemplo clássico de função recursiva e para mostrar que a parte recursiva de uma definição pode ser complicada.

3.7 CARDINALIDADE

Dois conjuntos, A e B, são ditos *equipotentes*, ou tendo o mesmo *número de elementos* ou a mesma *cardinalidade*, denotando-se por $A \sim B$, se existe uma correspondência um-a-um $f: A \to B$.

Um conjunto A é *finito* se A é vazio ou se A tem a mesma cardinalidade que o conjunto $\{1, 2, \ldots, n\}$ para algum inteiro positivo n. Um conjunto é *infinito* se não é finito. Exemplos familiares de conjuntos infinitos são os números naturais **N**, os inteiros **Z**, os números racionais **Q** e os números reais **R**.

Apresentamos agora a noção de "números cardinais". Vamos considerar números cardinais simplesmente como símbolos atribuídos a conjuntos de tal maneira que a dois conjuntos se atribui o mesmo símbolo se e somente se eles têm a mesma cardinalidade. O número cardinal de um conjunto A é comumente denotado por $|A|$, $n(A)$ ou $\text{card}(A)$. Usaremos $|A|$.

Usamos símbolos óbvios para os números cardinais de conjuntos finitos. Isto é, 0 é atribuído ao conjunto vazio $\varnothing$, e n é atribuído ao conjunto $\{1, 2, \ldots, n\}$. Portanto, $|A| = n$ se e somente se A tem a mesma cardinalidade que $\{1, 2, \ldots, n\}$, o que implica que A tem n elementos.

O número cardinal do conjunto infinito **N** dos inteiros positivos é $\aleph_0$ ("álefe-zero"). Este símbolo foi introduzido por Cantor. Logo, $|A| = \aleph_0$ se e somente se A tem a mesma cardinalidade de **N**.

Exemplo 3.9

(*a*) $|\{x, y, z\}| = 3$ e $|\{1, 3, 5, 7, 9\}| = 5$.

(*b*) Seja $E = \{2, 4, 6, \ldots\}$, o conjunto dos inteiros pares positivos. A função $f: \mathbf{N} \to E$ definida por $f(n) = 2n$ estabelece uma correspondência um-a-um entre os inteiros positivos **N** e E. Assim, E tem a mesma cardinalidade que **N** de forma que podemos escrever

$$|E| = \aleph_0$$

Um conjunto com cardinalidade $\aleph_0$ é dito *enumerável*†. Um conjunto finito ou enumerável é dito *contável*††. Pode-se mostrar que o conjunto **Q** dos números racionais é contável. De fato, temos o seguinte teorema (provado no Problema 3.15) que será usado posteriormente.

Teorema 3-2: a união contável de conjuntos contáveis é contável.

Em outras palavras, se $A_1, A_2, \ldots$ são conjuntos contáveis, então a união

$$A_1 \cup A_2 \cup A_3 \cup \cdots$$

também é um conjunto contável.

Um exemplo importante de um conjunto infinito e não contável, é dado pelo teorema seguinte, que está provado no Problema 3.16.

Teorema 3-3: o conjunto I de todos os números reais entre 0 e 1 é não contável.

Desigualdades e Números Cardinais

Deseja-se também comparar o tamanho de dois conjuntos. Isso é feito utilizando-se uma relação de desigualdade definida para números cardinais como a seguir. Para quaisquer conjuntos A e B, definimos $|A| \leq |B|$ se existe uma função $f: A \to B$ injetora. Escrevemos

$$|A| < |B| \qquad \text{se} \qquad |A| \leq |B| \qquad \text{mas} \qquad |A| \neq |B|$$

Por exemplo, $|\mathbf{N}| < |I|$, onde $I = \{x: 0 \leq x \leq 1\}$, já que a função $f: \mathbf{N} \to I$ definida por $f(n) = 1/n$ é injetora, mas $|\mathbf{N}| \neq |I|$ pelo Teorema 3.3.

O teorema de Cantor, enunciado a seguir e provado no Problema 3.28, nos diz que os números cardinais são não limitados.

Teorema 3-4 **(Cantor):** para qualquer conjunto A, temos $|A| < |\text{Partes}(A)|$ (onde Partes(A) é a coleção de todos os subconjuntos de A).

O próximo teorema nos diz que a relação de desigualdade para números cardinais é anti-simétrica.

Teorema 3-5 **(Schroeder-Bernstein):** suponha que A e B são conjuntos tais que

$$|A| \leq |B| \qquad \text{e} \qquad |B| \leq |A|$$

Então, $|A| = |B|$.

Mostramos uma fomulação equivalente deste teorema no Problema 3.29.

3.8 ALGORITMOS E FUNÇÕES

Um algoritmo M é uma lista finita de passos com instruções bem definidas para resolver um problema particular, quer dizer, para determinar a saída $f(X)$ de uma dada função f com entrada X (aqui, X pode ser uma lista ou conjunto de valores). Freqüentemente, pode existir mais de uma maneira de obter $f(X)$, como ilustrado pelos exemplos seguintes. A escolha particular do algoritmo M para obter $f(X)$ pode depender da "eficiência" ou "complexidade" do algoritmo; esta questão de complexidade do algoritmo M é discutida formalmente na seção seguinte.

Exemplo 3.10 (Avaliação de polinômios) Suponha que queremos determinar $f(a)$ para um polinômio $f(x)$ e um valor $x = a$ dados, a saber,

$$f(x) = 2x^3 - 7x^2 + 4x - 15 \qquad \text{e} \qquad a = 5$$

Isso pode ser feito de uma das duas maneiras a seguir.

† N. de T. No original, *denumerable* ou *countably infinite*.

†† N. de T. Grande parte dos textos em português não faz distinção entre conjuntos finitos e conjuntos com a cardinalidade de **N**, chamando ambos enumeráveis.

(*a*) (***Método direto***): substituímos $a = 5$ diretamente no polinômio para obter

$$f(5) = 2(125) - 7(25) + 4(5) - 7 = 250 - 175 + 20 - 15 = 80$$

Observe que existem $3 + 2 + 1 = 6$ multiplicações e três adições. Em geral, avaliar um polinômio de grau n diretamente vai requerer aproximadamente

$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2} \text{ multiplicações} \qquad \text{e} \qquad n \text{ adições}$$

(*b*) (***Método de Horner ou divisão sintética***): rescrevemos o polinômio colocando x em evidência (à direita) sucessivamente como a seguir:

$$f(x) = (2x^2 - 7x + 4)x - 15 = (((2x - 7)x + 4)x - 15$$

Então,

$$f(5) = ((3)5 + 4)5 - 15 = (19)5 - 15 = 95 - 15 = 80$$

Para os que estão familiarizados com divisão sintética, a aritmética acima é equivalente ao seguinte algoritmo de divisão sintética:

$$\begin{array}{r|rrrrrr} 5 & 2 & - & 7 & + & 4 & - & 15 \\ & & & 10 & + & 15 & + & 95 \\ \hline & 2 & + & 3 & + & 19 & + & 80 \end{array}$$

Observe que aqui existem três multiplicações e três adições. Em geral, a avaliação de um polinômio de grau n pelo método de Horner deve requerer aproximadamente

$$n \text{ multiplicações} \quad \text{e} \quad n \text{ adições}$$

Claramente, o método de Horner (*b*) é mais eficiente do que o método direto (*a*).

Exemplo 3.11 (Máximo divisor comum) Sejam a e b inteiros positivos com $b < a$; e suponha que queremos achar $d = \text{MDC}(a, b)$ o máximo divisor comum de a e b. Pode-se fazer isso das duas maneiras seguintes.

(*a*) (***Método direto***): achamos todos os divisores de a testando todos os números de 2 até $a/2$, e todos os divisores de b. Então escolhemos o maior divisor comum. Por exemplo, suponha $a = 258$ e $b = 60$. Os divisores de a e b são:

$a = 258$; divisores: 1, 2, 3, 6, 86, 129, 258
$b = 60$; divisores; 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Conseqüentemente, $d = \text{MDC}(258, 60) = 6$.

(*b*) (***Algoritmo de Euclides***): dividimos a por b para obter o resto r_1 (note que $r_1 < b$). Então dividimos b pelo resto r_1 para obter um segundo resto r_2 (note que $r_2 < r_1$). Depois dividimos r_1 por r_2 para obter um terceiro resto r_3 (note que $r_3 < r_2$). Continuamos dividindo r_k por r_{k+1} para obter o resto r_{k+2}. Como

$$a > b > r_1 > r_2 > r_3 \cdots \qquad (*)$$

por fim obtemos o resto $r_m = 0$. Então, $r_{m-1} = \text{MDC}(a, b)$. Por exemplo, suponha $a = 258$ e $b = 60$. Então:

(1) Dividindo $a = 258$ por $b = 60$, obtém-se o resto $r_1 = 18$.
(2) Dividindo $b = 60$ por $r_1 = 18$, obtém-se o resto $r_2 = 6$.
(3) Dividindo $r_1 = 18$ por $r_2 = 6$, obtém-se o resto $r_3 = 0$.

Portanto, $r_2 = 6 = \text{MDC}(258, 60)$.

O algoritmo de Euclides é uma maneira muito eficiente de achar o máximo divisor comum de dois inteiros positivos a e b. O fato de que o algoritmo termina, resulta de (*). O fato de que o algoritmo resulta em $d = \text{MDC}(a, b)$ não é óbvio; isso é discutido na Seção 11.6.

3.9 COMPLEXIDADE DE ALGORITMOS

A análise de algoritmos é uma tarefa fundamental na ciência da computação. Para comparar algoritmos, precisamos dispor de alguns critérios que medem sua eficiência. Esta seção discute esse importante tópico.

Suponha que M é um algoritmo, e n, o tamanho do dado de entrada. O tempo e o espaço usados pelo algoritmo são as duas medidas principais para a eficiência de M. O tempo é medido contando o número de "operações-chave"; por exemplo:

(*a*) Em processos de ordenação e busca, conta-se o número de operações.
(*b*) Em aritmética, contam-se multiplicações e adições são desprezadas.

Operações-chave são, portanto, definidas quando o tempo de execução das outras operações é muito menor ou, no máximo, proporcional ao tempo das operações-chave. O espaço é medido calculando o maior espaço de memória de que o algoritmo necessita.

A *complexidade* de um algoritmo M é a função $f(n)$ que calcula o tempo de execução e/ou o espaço de memória necessários para o algoritmo em função do tamanho n do dado de entrada. Freqüentemente o espaço de memória requerido por um algoritmo é simplesmente um múltiplo do tamanho do dado de entrada. Por conseguinte, a menos que seja feita ou esteja implícita uma especificação em contrário, o termo "complexidade"se refere ao tempo de execução do algoritmo.

A função de complexidade $f(n)$, que admitimos calcular o tempo de execução do algoritmo, normalmente depende não apenas do tamanho n do dado de entrada, mas também do tipo particular de dado. Por exemplo, suponha que queiramos fazer uma busca da primeira ocorrência de uma dada palavra de três letras W em uma história TEXT em inglês. Claramente, se W for a palavra "the", então é provável que W ocorra perto do início de TEXT, de tal maneira que $f(n)$ será pequena. Por outro lado, se W for a palavra "zoo", então W pode nem aparecer em TEXT, e $f(n)$ será grande.

A discussão acima nos leva à questão de determinar a função de complexidade $f(n)$ para alguns casos. Os dois casos normalmente investigados na teoria de complexidade são os seguintes:

(1) *Pior caso*: o maior valor possível de $f(n)$ para qualquer dado de entrada.
(2) *Caso médio*: o valor esperado de $f(n)$.

A análise do caso médio pressupõe certa distribuição probabilística para o dado de entrada; uma hipótese possível é a de que as permutações do conjunto de dados são igualmente prováveis. O caso médio também utiliza o conceito seguinte da teoria de probabilidades. Suponha que os números $n_1, n_2, \ldots, n_k$ ocorram com, respectivamente, as probabilidades $p_1, p_2, \ldots, p_k$. A *expectância* ou *valor médio* E é dado por

$$E = n_1p_1 + n_2p_2 + \ldots + n_kp_k$$

Estas idéias estão ilustradas a seguir.

Busca Linear

Suponha que um *array* linear DATA contenha n elementos, e suponha que um ITEM específico de informação seja dado. Queremos ou achar a localização LOC de ITEM no *array* DATA, ou enviar alguma mensagem, tal como LOC = 0, para indicar que ITEM não aparece em DATA. O algoritmo de busca linear resolve este problema comparando, um a um, cada elemento de DATA com ITEM. Isto é, comparamos ITEM com DATA[1], depois DATA[2], e assim por diante, até acharmos LOC tal que ITEM = DATA[LOC].

A complexidade do algoritmo de busca é dada pelo número C de comparações entre ITEM e DATA[K]. Determinamos $C(n)$ para o pior caso e para o caso médio.

(1) *Pior caso*: claramente o pior caso ocorre quando ITEM é o último elemento do *array* DATA ou não está no *array*. Em qualquer das situações, temos

$$C(n) = n$$

Conseqüentemente, $C(n) = n$ é a complexidade do pior caso para o algoritmo de busca linear.

(2) *Caso médio*: aqui assumimos que ITEM está em DATA e que aparece em qualquer uma das posições com a mesma probabilidade. Conseqüentemente, o número de comparações pode ser qualquer número entre 1,2,3..., n, e cada número ocorre com probabilidade $p = 1/n$.

Então:

$$\begin{aligned} C(n) &= 1 \cdot \frac{1}{n} + 2 \cdot \frac{1}{n} + \cdots + n \cdot \frac{1}{n} \\ &= (1 + 2 + \cdots + n) \cdot \frac{1}{n} \\ &= \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2} \end{aligned}$$

O resultado é compatível com a nossa intuição de que o número médio de comparações necessárias para achar a localização de ITEM é igual à metade do número de elementos da lista DATA.

Nota: A complexidade do caso médio de um algoritmo é normalmente muito mais complicada de analisar do que a do pior caso. Ademais, a distribuição probabilística assumida para o caso médio pode não ser adequada a situações reais. Conseqüentemente, a menos que seja feita ou esteja implícita uma afirmação em contrário, a complexidade de um algoritmo é a função que determina o tempo de execução do pior caso em termos do tamanho do dado de entrada. Esta não é uma hipótese muito restritiva, uma vez que a complexidade do caso médio para muitos algoritmos é proporcional ao pior caso.

Taxa de Crescimento e Notação *O*

Suponha que M seja um algoritmo e que n seja o tamanho do dado de entrada. Claramente a complexidade $f(n)$ de M aumenta quando n aumenta. Normalmente queremos examinar a razão de crescimento de $f(n)$. Isto, em geral, é feito comparando $f(n)$ com algumas funções padrão, tais como

$$\log_2 n, \quad n, \quad n \log_2 n, \quad n^2, \quad n^3, \quad 2^n$$

As taxas de crescimento para essas funções-padrão estão indicadas na Figura 3-6, que informa seus valores aproximados para alguns valores de n. Observe que as funções estão listadas na ordem das suas taxas de crescimento: a função logarítmica $\log_2 n$ cresce mais lentamente, a função exponencial cresce mais rapidamente, e as funções polinomiais n^c crescem de acordo com o grau do polinômio c.

n \ $g(n)$	$\log n$	n	$n \log n$	n^2	n^3	2^n
5	3	5	15	25	125	32
10	4	10	40	100	10^3	10^3
100	7	100	700	10^4	10^6	10^{30}
1000	10	10^3	10^4	10^6	10^9	10^{300}

Taxa de crescimento das funções-padrão.

Fig. 3-6

A maneira pela qual comparamos a função de complexidade $f(n)$ com uma das funções-padrão utiliza a notação O, formalmente definida a seguir.

Definição: Sejam $f(x)$ e $g(x)$ funções arbitrárias definidas em **R** ou em um subconjunto de **R**. Dizemos que "$f(x)$ é da ordem de $g(x)$", escrevendo

$$f(x) = O(g(x))$$

se existem um número real k e uma constante positiva C tais que, para todo $x > k$, temos

$$|f(x)| \leq C|g(x)|$$

Também escrevemos

$$f(x) = h(x) + O(g(x)) \qquad \text{quando} \qquad f(x) - h(x) = O(g(x))$$

(A notação acima é conhecida como notação "*big O*", já que $f(x) = o(g(x))$ tem um significado inteiramente diferente.)

Considere agora o polinômio $P(x)$ de grau m. Mostramos no Problema 3.27 que $P(x) = O(x^m)$. Logo, por exemplo,

$$7x^2 - 9x + 4 = O(x^2) \qquad \text{e} \qquad 8x^3 - 576x^2 + 832x - 248 = O(x^3)$$

Complexidade de Algoritmos Tradicionais

Assumindo que $f(n)$ e $g(n)$ são funções definidas nos inteiros positivos, então

$$f(n) = O(g(n))$$

significa que $f(n)$ é limitada por um múltiplo constante de $g(n)$ para quase todo n.

Para exemplificar a conveniência desta notação, damos a complexidade de alguns algoritmos de busca e ordenação bem conhecidos na ciência da computação:

(*a*) Busca linear: $O(n)$
(*b*) Busca binária: $O(\log n)$
(*c*) *Bubble-sort*: $O(n^2)$
(*d*) *Merge-sort*: $O(n \log n)$

Problemas Resolvidos

Funções

3.1 Diga se cada um dos diagramas na Figura 3-7 define uma função de $A = \{a, b, c\}$ em $B = \{x, y, z\}$.

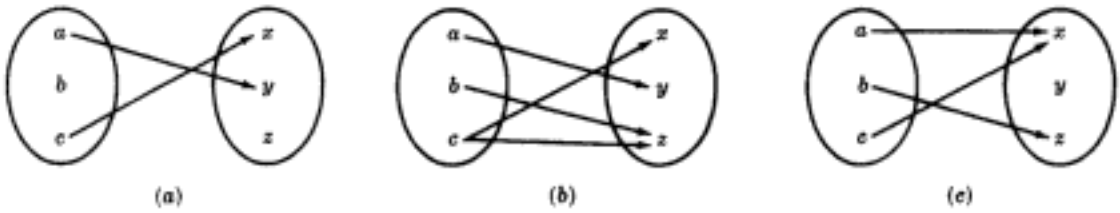


Fig. 3-7

(*a*) Não. Não existe nada associado ao elemento $b \in A$
(*b*) Não. Dois elementos, x e z, estão associados a $c \in A$.
(*c*) Sim.

3.2 Seja $X = \{1, 2, 3, 4\}$ Determine se cada uma das relações abaixo é uma função de X em X.

(*a*) $f = \{(2,3), (1,4), (2,1)(3,2), (4,4)\}$.
(*b*) $g = \{(3,1), (4,2), (1,1)\}$.
(*c*) $h = \{(2,1), (3,4), (1,4), (2,1), (4,4)\}$.

Lembre que um subconjunto f de $X \times X$ é uma função $f: X \to X$ se e somente se cada $a \in X$ aparece como primeira coordenada em exatamente um par ordenado em f.

(*a*) Não. Dois pares ordenados (2,3) e (2,1) em f têm o mesmo número 2 como primeira coordenada.
(*b*) Não. O elemento $2 \in X$ não aparece como primeira coordenada em nenhum par ordenado em g.
(*c*) Sim. Embora $2 \in X$ apareça como primeira coordenada de dois pares ordenados em h, esses dois pares ordenados são iguais.

3.3 Seja A o conjunto de estudantes de uma escola. Determine quais das seguintes associações define uma função em A.

(*a*) A cada estudante, associe sua idade.
(*b*) A cada estudante, associe seu professor.
(*c*) A cada estudante, associe seu sexo.
(*d*) A cada estudante, associe seu cônjuge.

Uma coleção de associações é uma função em A se e somente se cada elemento de A está associado a exatamente um elemento. Assim:

(*a*) Sim, porque cada estudante tem uma e apenas uma idade.

(*b*) Sim, se cada estudante tem apenas um professor; não, se algum estudante tem mais do que um professor.

(*c*) Sim.

(*d*) Não, se algum estudante não for casado; sim, caso contrário.

3.4 Esboce o gráfico de:

(*a*) $f(x) = x^2 + x - 6$ (*b*) $g(x) = x^3 - 3x^2 - x + 3$

Organize uma tabela de valores de x e então ache os valores correspondentes da função. Como as funções são polinomiais, plote os pontos em um plano cartesiano e desenhe uma curva suave unindo-os. Veja a Figura 3-8.

x	$f(x)$
−4	6
−3	0
−2	−4
−1	−6
0	−6
1	−4
2	0
3	6

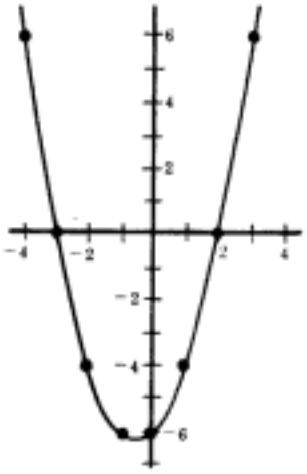


Gráfico de f

x	$g(x)$
−2	−15
−1	0
0	3
1	0
2	−3
3	0
4	15

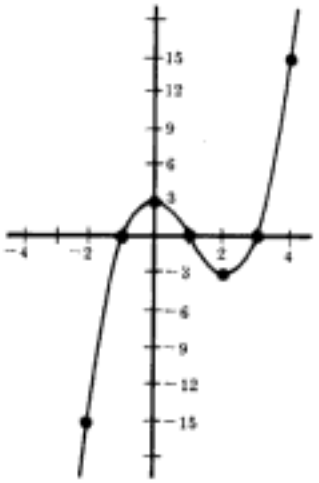


Gráfico de g

Fig. 3-8

3.5 Considere as funções $f: A \to B$ e $g: B \to C$ definidas pela Figura 3-9. Ache a função composta $g \circ f: A \to C$

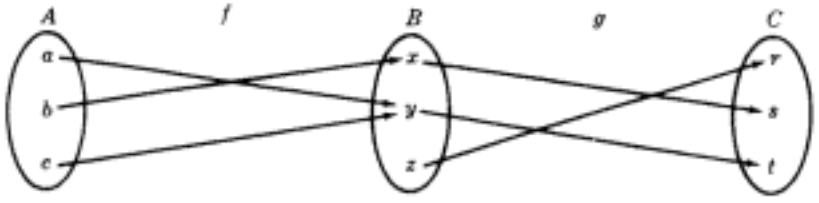


Fig. 3-9

Usamos a definição de função composta para calcular:

$$(g \circ f)(a) = g(f(a)) = g(y) = t$$
$$(g \circ f)(b) = g(f(b)) = g(x) = s$$
$$(g \circ f)(c) = g(f(c)) = g(y) = t$$

Note que chegamos à mesma resposta que se tivéssemos "seguido as setas" no diagrama:

$$a \to y \to t, \qquad b \to x \to s, \qquad c \to y \to t$$

3.6 Considere as funções f e g definidas por $f(x) = 2x + 1$ e $g(x) = x^2 - 2$. Ache a fórmula que define a função composta $g \circ f$.

Compute $g \circ f$ como a seguir: $(g \circ f) = g(f(x)) = g(2x + 1) = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$.

Observe que a mesma resposta pode ser obtida escrevendo:

$$y = f(x) = 2x + 1 \qquad \text{e} \qquad z = g(y) = y^2 - 2$$

e então eliminando y de ambas as equações:

$$z = y^2 - 2 = (2x + 1)^2 - 2 = 4x^2 + 4x - 1$$

Funções Injetoras, Sobrejetoras e Inversíveis

3.7 Determine se cada uma das funções é injetora.

(*a*) A cada pessoa na Terra, associe o número correspondente à sua idade.

(*b*) A cada país no mundo, associe a latitude e a longitude de sua capital.

(*c*) A cada livro escrito por um único autor, associe o autor.

(*d*) A cada país no mundo que tem um primeiro-ministro, associe o primeiro-ministro.

(*a*) Não. Muitas pessoas no mundo têm a mesma idade.

(*b*) Sim.

(*c*) Não. Existem livros diferentes com um mesmo autor.

(*d*) Sim. Países diferentes no mundo têm primeiros-ministros diferentes.

3.8 Considere as funções $f: A \to B$, $g: B \to C$ e $h: C \to D$ definidas na Figura 3-10.

(*a*) Determine se cada função é sobrejetora.

(*b*) Ache a função composta $h \circ g \circ f$.

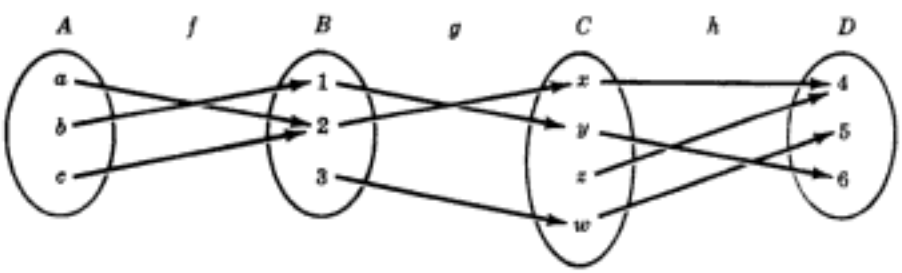


Fig. 3-10

(*a*) A função $f: A \to B$ não é sobrejetora já que $3 \in B$ não é imagem de nenhum elemento em A.

A função $g: B \to C$ não é sobrejetora já que $z \in C$ não é imagem de nenhum elemento em B.

A função $h: C \to D$ é sobrejetora já que cada elemento em D é a imagem de algum elemento de C.

(*b*) Agora, $a \to 2 \to x \to 4$, $b \to 1 \to y \to 6$, $c \to 2 \to x \to 4$. Portanto, $h \circ g \circ f = \{(a, 4), (b, 6), (c, 4)\}$.

3.9 Considere as funções $f: A \to B$ e $g: B \to C$. Prove o seguinte:

(*a*) Se f e g são injetoras, então a função composta $g \circ f$ é injetora.

(*b*) Se f e g são sobrejetoras, então $g \circ f$ é sobrejetora.

(*a*) Suponha $(g \circ f)(x) = (g \circ f)(y)$; então, $(g(f(x)) = (g(f(y))$. Portanto, $f(x) = f(y)$ porque g é injetora. Além do mais, $x = y$ porque f é injetora. Conseqüentemente, $g \circ f$ é injetora.

(*b*) Seja c um elemento arbitrário de C. Como g é sobrejetora, existe um $b \in B$ tal que $g(b) = c$. Como f é sobrejetora, existe um $a \in A$, tal que $f(a) = b$. Mas neste caso,

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

Portanto, cada $c \in C$ é a imagem de algum elemento $a \in A$. Conseqüentemente, $g \circ f$ é uma função sobrejetora.

3.10 Seja f: $\mathbf{R} \to \mathbf{R}$ definida por $f(x) = 2x - 3$. Assim, f é injetora e sobrejetora e, portanto, f tem uma função inversa f^{-1}. Ache uma fórmula para f^{-1}.

Seja y a imagem de x pela função f:

$$y = f(x) = 2x - 3$$

Conseqüentemente, x é a imagem de y pela função inversa f^{-1}. Calcule x em função de y na equação acima:

$$x = (y + 3)/2$$

Então, $f^{-1}(y) = (y + 3)/2$. Troque y por x para obter

$$f^{-1}(x) = \frac{x + 3}{2}$$

que é a fórmula para f^{-1} usando a variável independente usual x.

3.11 Prove a seguinte generalização da lei de DeMorgan: para qualquer classe de conjuntos, temos

$$(\cup_i A_i)^c = \cap_i A_i^c$$

Temos:

$$x \in (\cup_i A_i)^c \quad \text{sse} \quad x \notin \cup_i A_i, \quad \text{sse} \quad \forall_i \in I, x \notin A_i, \quad \text{sse} \quad \forall_i \in I, x \in A_i^c, \quad \text{sse} \quad x \in \cap_i A_i^c$$

Portanto, $(\cup_i A_i)^c = \cap_i A_i^c$. (Aqui, usamos a notação "sse" para "se e somente se" e $\forall$ para "para qualquer".)

Cardinalidade

3.12 Ache o número cardinal de cada conjunto.

(*a*) $A = \{a, b, c, \ldots, y, z\}$ (*d*) $D = \{10, 20, 30, 40, \ldots\}$

(*b*) $B = \{1, -3, 5, 11, -28\}$ (*e*) $E = \{6, 7, 8, 9, \ldots\}$

(*c*) $C = \{x: x \in \mathbf{N}, x^2 = 5\}$

(*a*) $|A| = 26$, uma vez que existem 26 letras no alfabeto.

(*b*) $|B| = 5$.

(*c*) $|C| = 0$, já que não existe inteiro positivo cujo quadrado seja 5. I.e., C é vazio.

(*d*) $|D| = \aleph_0$, porque f: $\mathbf{N} \to D$, definida por $f(n) = 10n$, é uma correspondência um-a-um entre $\mathbf{N}$ e D.

(*e*) $|E| = \aleph_0$, porque g: $\mathbf{N} \to E$, definida por $g(n) = n + 5$, é uma correspondência um-a-um entre $\mathbf{N}$ e E.

3.13 Mostre que o conjunto $\mathbf{Z}$ dos inteiros tem cardinalidade $\aleph_0$.

O seguinte diagrama mostra uma correspondência um-a-um entre $\mathbf{N}$ e $\mathbf{Z}$:

$$\begin{array}{lcccccccccc} \mathbf{N} = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\ \mathbf{Z} = & 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \ldots \end{array}$$

Isto é, a seguinte função f: $\mathbf{N} \to \mathbf{Z}$ é injetora e sobrejetora:

$$f(n) = \begin{cases} n/2 & \text{se } n \text{ é par} \\ (1 - n)/2 & \text{se } n \text{ é ímpar} \end{cases}$$

Conseqüentemente, $|\mathbf{Z}| = |\mathbf{N}| = \aleph_0$.

3.14 Sejam $A_1, A_2, \ldots$ um número contável de conjuntos finitos. Mostre que $S = \cup_i A_i$ é contável.

Essencialmente, listamos os elementos de A_1, depois listamos os elementos de A_2 que não pertencem a A_1, e então listamos os elementos de A_3 que não pertencem a A_1 ou A_2, i.e., que ainda não estão na lista, e assim por diante. Como A_1 é finito, sempre se pode listar os elementos de cada conjunto.

Primeiramente definimos conjuntos $B_1, B_2, \ldots$ onde B_i contém os elementos de A_i que não pertencem aos conjuntos precedentes, i.e., definimos

$$B_1 = A_1 \qquad \text{e} \qquad B_k = A_k \backslash (A_1 \cup A_2 \cup \cdots \cup A_{k-1})$$

Então, os B_i são disjuntos e $S = \cup_i B_i$. Sejam $b_{i1}, b_{i2}, \ldots b_{im_i}$ os elementos de B_i. Então, $S = \{b_{ij}\}$. Seja f: $S \to \mathbf{N}$ definida como a seguir:

$$f(b_{ij}) = m_1 + m_2 + \cdots + m_{i-1} + j$$

Se S é finito, então S é contável. Se S é infinito, então f é uma correspondência um-a-um entre S e $\mathbf{N}$. Logo, S é contável.

3.15 Prove o Teorema 3.2: a união contável de conjuntos contáveis é contável.

Suponha que $A_1, A_2, A_3, \ldots$ é um número contável de conjuntos contáveis. Em particular, suponha que $a_1, a_2, a_3, \ldots$ são elementos de A_i. Defina conjuntos $B_2, B_3, B_4, \ldots$ como a seguir:

$$B_k = \{a_{ij}: i + j = k\}$$

Por exemplo, $B_6 = \{a_{15}, a_{24}, a_{33}, a_{42}, a_{51}\}$. Observe que cada B_k é finito e

$$S = \cup_i A_i = \cup_k B_k$$

Pelo problema precedente, $\cup_k B_k$ é contável. Logo, $S = \cup_i A_i$ é contável, e o Teorema está provado.

3.16 Prove o Teorema 3.3: o conjunto $\boldsymbol{I}$ dos números reais entre 0 e 1, inclusive, é não contável.

O conjunto $\boldsymbol{I}$ é claramente infinito, já que contém $1, \frac{1}{2}, \frac{1}{3}, \ldots$ Suponha que $\boldsymbol{I}$ é enumerável. Então, existe uma correspondência um-a-um f: $\mathbf{N} \to \boldsymbol{I}$. Seja $f(1) = a_1, f(2) = a_2, \ldots$; isto é, $I = \{a_1, a_2, a_3, \ldots\}$. Listamos os elementos $a_1, a_2, \ldots$ em colunas e expressamos cada um pela sua expansão decimal:

$$\begin{aligned} a_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ a_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ a_3 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ a_4 &= 0.x_{41}x_{42}x_{43}x_{44}\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

onde $x_{ij} \in \{0, 1, 2, \ldots, 9\}$. (Para os números que podem ser expressos em duas expansões decimais distintas, por exemplo, 0,2000000... = 0,1999999..., escolhemos a expansão que termina com noves.)

Seja $b = 0.y_1y_2y_3y_4\ldots$ o número real obtido como a seguir:

$$y_j = \begin{cases} 1 & \text{se } x_{jj} \neq 1 \\ 2 & \text{se } x_{jj} = 1 \end{cases}$$

Agora, $b \in \boldsymbol{I}$. Mas,

$$\begin{aligned} &b \neq a_1 \text{ porque } y_1 \neq x_{11} \\ &b \neq a_2 \text{ porque } y_2 \neq x_{22} \\ &b \neq a_3 \text{ porque } y_3 \neq x_{33} \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Portanto, b não pertence a $I = \{a_1, a_2, \ldots\}$. Isso contradiz o fato de que $b \in \boldsymbol{I}$. Logo, a hipótese de que $\boldsymbol{I}$ é enumerável é falsa; portanto, $\boldsymbol{I}$ é não contável.

Funções Matemáticas Especiais

3.17 Ache: (*a*) $\lfloor 7{,}5 \rfloor$; $\lfloor -7{,}5 \rfloor, \lfloor -18 \rfloor$; (*b*) $\lceil 7{,}5 \rceil, \lceil -7{,}5 \rceil, \lceil -18 \rceil$.

(*a*) Por definição, $\lfloor x \rfloor$ denota o maior inteiro que não excede x; logo, $\lfloor 7{,}5 \rfloor = 7, \lfloor -7{,}5 \rfloor = -8, \lfloor -18 \rfloor = -18$.

(*b*) Por definição, $\lceil x \rceil$ denota o menor inteiro que não é menor do que x; logo, $\lceil 7{,}5 \rceil = 8, \lceil -7{,}5 \rceil = -7, \lceil -18 \rceil = -18$.

3.18 Ache: (*a*) $25 \pmod 7$; (*b*) $25 \pmod 5$; (*c*) $-35 \pmod{11}$; (*d*) $-3 \pmod 8$.

Quando k é positivo, simplesmente divida k pelo *modulus* M para obter o resto r. Então, $r \equiv k \pmod M$. Se k é negativo, divida $|k|$ por M para obter o resto r'. Então, $k \pmod M \equiv M - r'$ (quando $r' \neq 0$). Logo:

(*a*) $25 \pmod 7 = 4$, (*c*) $-35 \pmod{11} = 11 - 2 = 9$,

(*b*) $25 \pmod 5 = 0$, (*d*) $-3 \pmod 8 = 8 - 3 = 5$.

3.19 Usando aritmética módulo $M = 15$, avalie: (*a*) $9 + 13$; (*b*) $7 + 11$; (*c*) $4 - 9$; (*d*) $2 - 10$.

Use $a + M \equiv a \pmod M$:

(*a*) $9 + 13 = 22 \equiv 22 - 15 = 7$. (*c*) $4 - 9 = -5 \equiv -5 + 15 = 10$.

(*b*) $7 + 11 = 18 \equiv 18 - 15 = 3$. (*d*) $2 - 10 = -8 \equiv -8 + 15 = 7$.

3.20 Simplifique: (*a*) $\dfrac{n!}{(n-1)!}$; (*b*) $\dfrac{(n+2)!}{n!}$.

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$ ou, simplesmente, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n$.

(*b*) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = (n+2)(n+1) = n^2 + 3n + 2$

ou, simplesmente, $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2$.

3.21 Avalie: (*a*) $\log_2 8$; (*b*) $\log_2 64$; (*c*) $\log_{10} 100$; (*d*) $\log_{10} 0{,}001$.

(*a*) $\log_2 8 = 3$, já que $2^3 = 8$. (*c*) $\log_{10} 100 = 2$, já que $10^2 = 100$.

(*b*) $\log_2 64 = 6$, já que $2^6 = 64$. (*d*) $\log_{10} 0{,}001 = -3$, já que $10^{-3} = 0{,}001$.

Observação: Freqüentemente, logaritmos são expressos usando valores aproximados. Por exemplo, usando tabelas ou calculadoras, obtemos

$$\log_{10} 300 = 2{,}4771 \qquad \text{e} \qquad \log_e 40 = 3{,}6889$$

como respostas aproximadas. (Aqui, $e = 2{,}718281\ldots$)

Funções Recursivas

3.22 Sejam a e b inteiros positivos e suponha que Q é definida recursivamente como a seguir:

$$Q(a,b) = \begin{cases} 0 & \text{se } a < b \\ Q(a-b,b) + 1 & \text{se } b \leq a \end{cases}$$

(*a*) Ache: (i) $Q(2, 5)$, (ii) $Q(12, 5)$

(*b*) O que faz a função Q? Ache $Q(5861,7)$.

(*a*) (i) $Q(2, 5) = 0$, já que $2 < 5$.

(ii) $Q(12, 5) = Q(7, 5) + 1$
$= [Q(2, 5) + 1] + 1 = Q(2, 5) + 2$
$= 0 + 2 = 2$

(*b*) Cada vez que b é subtraído de a, o valor de Q aumenta em 1. Portanto, $Q(a, b)$ determina o quociente da divisão de a por b. Assim, $Q(5861, 7) = 837$.

3.23 Seja n um inteiro positivo. Suponha que a função L é definida recursivamente como a seguir:

$$L(n) = \begin{cases} 0 & \text{se } n = 1 \\ L(\lfloor n/2 \rfloor) + 1 & \text{se } n > 1 \end{cases}$$

Ache $L(25)$ e descreva o que a função faz.

Ache $L(25)$ recursivamente como a seguir:

$$\begin{aligned} L(25) &= L(12) + 1 \\ &= [L(6) + 1] + 1 = L(6) + 2 \\ &= [L(3) + 1] + 2 = L(3) + 3 \\ &= [L(1) + 1] + 3 = L(1) + 4 = 0 + 4 = 4 \end{aligned}$$

Cada vez que n é dividido por 2, o valor de L é acrescido de 1. Portanto, L é o maior inteiro tal que

$$2^L \leq n$$

Conseqüentemente, $$L(n) = \lfloor \log_2 n \rfloor$$

3.24 Use a definição da função de Ackermann para achar $A(1, 3)$.

Temos os 15 passos seguintes:

(1) $A(1,3) = A(0, A(1,2))$
(2) $A(1,2) = A(0, A(1,1))$
(3) $A(1,1) = A(0, A(1,0))$
(4) $A(1,0) = A(0,1)$
(5) $A(0,1) = 1 + 1 = 2$
(6) $A(1,0) = 2$
(7) $A(1,1) = A(0,2)$
(8) $A(0,2) = 2 + 1 = 3$
(9) $A(1,1) = 3$
(10) $A(1,2) = A(0,3)$
(11) $A(0,3) = 3 + 1 = 4$
(12) $A(1,2) = 4$
(13) $A(1,3) = A(0,4)$
(14) $A(0,4) = 4 + 1 = 5$
(15) $A(1,3) = 5$

A tabulação deslocada para frente indica que estamos adiando uma avaliação e chamando a definição novamente, e a tabulação deslocada para trás indica que estamos retornando o processo. Observe que a parte (*a*) da definição é usada nos Passos 5, 8, 11 e 14; (*b*) no Passo 4; e (*c*) nos Passos 1, 2 e 3. Nos outros passos, estamos retornando o processo fazendo substituições.

Problemas Variados

3.25 Ache o domínio D de cada uma das seguintes funções reais de uma variável real:

(*a*) $f(x) = \dfrac{1}{x-2}$ (*c*) $f(x) = \sqrt{25 - x^2}$

(*b*) $f(x) = x^2 - 3x - 4$ (*d*) $f(x) = x^2$ onde $0 \leq x \leq 2$

Quando uma função real de variável real é dada pela fórmula $f(x)$, o domínio D consiste, a menos de especificação em contrário, no maior subconjunto de $\mathbf{R}$ para o qual $f(x)$ faz sentido e é real.

(*a*) f não é definida para $x - 2 = 0$, i.e., para $x = 2$; portanto, $D = \mathbf{R} \setminus \{2\}$.

(*b*) f é definida para todo número real; portanto, $D = \mathbf{R}$.

(*c*) f não é definida quando $25 - x^2$ é negativo; portanto, $D = [-5, 5] = \{x : -5 \leq x \leq 5\}$.

(*d*) Aqui, o domínio de f é explicitamente dado por $D = \{x: 0 \leq x \leq 2\}$.

3.26 Para algum $n \in \mathbf{N}$, seja $D_n = (0, 1/n)$ o intervalo aberto entre 0 e $1/n$. Ache:

$$(a)\ D_3 \cup D_7; \quad (b)\ D_3 \cap D_{20}; \quad (c)\ D_s \cup D_t; \quad (d)\ D_s \cap D_t.$$

(*a*) Como $(0, 1/3)$ contém $(0, 1/7)$, $D_3 \cup D_7 = D_3$.

(*b*) Como $(0, 1/20)$ é um subconjunto de $(0, 1/3)$, $D_3 \cap D_{20} = D_{20}$.

(*c*) Seja $m = \min(s,t)$, isto é, o menor dos dois números s e t; então D_m é igual a D_s ou D_t e contém o outro como subconjunto. Portanto, $D_s \cup D_t = D_m$.

(*d*) Seja $M = \max(s, t)$, isto é, o maior entre os dois números s e t; então, $D_s \cap D_t = D_M$.

3.27 Suponha que $P(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_m n^m$ tem grau m. Prove $P(n) = O(n^m)$.

Seja $b_0 = |a_0|, b_1 = |a_1|, \ldots, b_m = |a_m|$. Então, para $n \geq 1$,

$$\begin{aligned} P(n) &\leq b_0 + b_1 n + b_2 n^2 + \cdots + b_m n^m = \left(\frac{b_0}{n^m} + \frac{b_1}{n^{m-1}} + \cdots + b_m\right) n^m \\ &\leq (b_0 + b_1 + \cdots + b_m) n^m = M n^m \end{aligned}$$

onde $M = |a_0| + |a_1| + \cdots + |a_m|$. Portanto, $P(n) = O(n^m)$.

Por exemplo, $5x^3 + 3x = O(x^3)$, e $x^5 - 4.000.000x^2 = O(x^5)$.

3.28 Prove o Teorema 3.4 (Cantor): $|A| < |\text{Partes}(A)|$ (onde Partes(A) é o conjunto de todos os subconjuntos de A).

A função $g: A \to \text{Partes}(A)$ definida por $g(a) = \{a\}$ é claramente injetora. Portanto, $|A| \leq |\text{Partes}(A)|$.

Se mostrarmos $|A| \neq |\text{Partes}(A)|$, o teorema fica provado. Suponha que não, isto é, que $|A| = |\text{Partes}(A)|$ e que $f: A \to \text{Partes}(A)$ é uma função injetora e sobrejetora. Denomine como elemento "ruim" um valor $a \in A$ tal que $a \notin f(a)$, e seja B o conjunto de elementos ruins. Em outras palavras,

$$B = \{x: x \in A,\ x \notin f(x)\}$$

B é um subconjunto de A. Como $f: A \to \text{Partes}(A)$ é sobrejetora, existe $b \in A$ tal que $f(b) = B$. b é ou não um elemento "ruim"? Se $b \in B$, então, pela definição de B, $b \notin f(b) = B$, o que é impossível. Do mesmo modo, se $b \notin B$, então $b \in f(b) = B$, o que também é impossível. Logo, a hipótese original de que $|A| = |\text{Partes}(A)|$ levou a uma contradição. Portanto, a hipótese é falsa e, logo, o teorema é verdadeiro.

3.29 Prove a seguinte formulação equivalente à do Teorema 3.5, de Schroeder-Bernstein: suponha $X \supseteq Y \supseteq X_1$ e $X \simeq X_1$. Então, $X \simeq Y$.

Como $X \simeq X_1$, existe uma correspondência um-a-um (bijeção) $f: X \to X_1$. Como $X \supseteq Y$, a restrição de f a Y, que também denotamos por f, também é um-a-um. Seja $f(Y) = Y_1$. Então, Y e Y_1 são equipotentes,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1$$

e $f: Y \to Y_1$ é bijetiva. Mas agora, $Y \supseteq X_1 \supseteq Y_1$ e $Y \simeq Y_1$. Por razões similares, X_1 e $f(X_1) = X_2$ são equipotentes,

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2$$

e $f: Y_1 \to Y_2$ é bijetiva. Conseqüentemente, existem conjuntos equipotentes $X, X_1, X_2, \ldots$ e conjuntos equipotentes $Y, Y_1, Y_2, \ldots$ tais que

$$X \supseteq Y \supseteq X_1 \supseteq Y_1 \supseteq X_2 \supseteq Y_2 \supseteq X_3 \supseteq Y_3 \supseteq \cdots$$

e $f: X_k \to X_{k+1}$ e $f: Y_k \to Y_{k+1}$ são bijetivas.

Seja

$$B = X \cap Y \cap X_1 \cap Y_1 \cap X_2 \cap Y_2 \cap \cdots$$

Então,

$$\begin{aligned} X &= (X \setminus Y) \cup (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup \cdots \cup B \\ Y &= (Y \setminus X_1) \cup (X_1 \setminus Y_1) \cup (Y_1 \setminus X_2) \cup \cdots \cup B \end{aligned}$$

Ademais, $X\backslash Y$, $X_1\backslash Y_1$, $X_2\backslash Y_2$, ... são equipotentes. De fato, a função

$$f\colon (X_k\backslash Y_k) \to (X_{k+1}\backslash Y_{k+1})$$

é injetora e sobrejetora.

Considere a função $g\colon X \to Y$ definida pelo diagrama da Figura 3-11. Isto é,

$$g(x) = \begin{cases} f(x) & \text{se } x \in X_k\backslash Y_k \text{ ou } x \in X\backslash Y \\ x & \text{se } x \in Y_k\backslash X_k \text{ ou } x \in B \end{cases}$$

Então g é injetora e sobrejetora. Portanto, $X \simeq Y$.

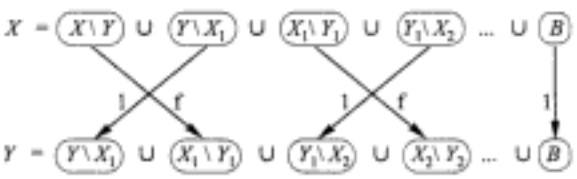


Fig. 3-11

Problemas Complementares

Funções

3.30 Seja $W = \{a, b, c, d\}$. Determine se cada conjunto de pares ordenados define uma função de W em W.

(*a*) $\{(b,a),(c,d),(d,a),(c,d),(a,d)\}$ (*c*) $\{(a,b),(b,b),(c,b),(d,b)\}$

(*b*) $\{(d,d),(c,a),(a,b),(d,b)\}$ (*d*) $\{(a,a),(b,a),(a,b),(c,d)\}$

3.31 Considere a função g que associa a cada nome na lista {Carla, Marcos, Maria, Nina, Fabiana} o número de letras necessárias para soletrar o nome. Descreva g como um conjunto de pares ordenados.

3.32 Seja $W = \{1, 2, 3, 4\}$ e seja $g\colon W \to W$ definida pela Figura 3-12. (*a*) Descreva g como um conjunto de pares ordenados. (*b*) Determine a imagem de g. (*c*) Escreva a função composta $g \circ g$ como um conjunto de pares ordenados.

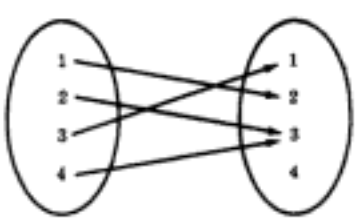


Fig. 3-12

3.33 Seja $V = \{1, 2, 3, 4\}$ e sejam

$$f = \{(1,3),(2,1),(3,4),(4,3)\} \quad \text{e} \quad g = \{(1,2),(2,3),(3,1),(4,1)\}$$

Ache: (*a*) $f \circ g$; (*b*) $g \circ f$; (*c*) $f \circ f$.

3.34 Seja $f\colon \mathbf{R} \to \mathbf{R}$ definida por $f(x) = 3x - 7$. Ache uma fórmula para a função inversa $f^{-1}\colon \mathbf{R} \to \mathbf{R}$.

Propriedades de Funções

3.35 Prove: se $f\colon A \to B$ e $g\colon B \to A$ satisfazem $g \circ f = 1_A$, então f é injetora e g é sobrejetora.

3.36 Prove o Teorema 3.1: uma função $f\colon A \to B$ é inversível se e somente se f é injetora e sobrejetora.

3.37 Prove: se $f\colon A \to B$ é inversível com função inversa $f^{-1}\colon B \to A$, então $f^{-1} \circ f = 1_A$ e $f \circ f^{-1} = 1_B$.

3.38 Para cada inteiro positivo n em $\mathbf{N}$, seja A_n o seguinte subconjunto dos números reais $\mathbf{R}$:

$$A_n = (0, 1/n) = \{x: 0 < x < 1/n\}$$

Ache: (*a*) $A_2 \cup A_5$ (*c*) $\cup(A_i: i \in J)$ (*e*) $\cup(A_i: i \in K)$
(*b*) $A_3 \cap A_7$ (*d*) $\cap(A_i: i \in J)$ (*f*) $\cap(A_i: i \in K)$

onde J é um subconjunto finito de $\mathbf{N}$, e K é um subconjunto infinito de $\mathbf{N}$.

3.39 Considere uma classe indexada de conjuntos $\{A_i: i \in I\}$, um conjunto B e um índice i_0 em I. Prove:

(*a*) $B \cap (\cup_i A_i) = \cup_i (B \cap A_i)$ (*b*) $\cap(A_i: i \in I) \subseteq A_{i_0} \subseteq \cup(A_i: i \in I)$

3.40 Para cada inteiro positivo n em $\mathbf{N}$, seja D_n o seguinte subconjunto de $\mathbf{N}$:

$$D_n = \{n, 2n, 3n, 4n, \ldots\} = \{\text{múltiplos de } n\}$$

(*a*) Ache (1) $D_2 \cap D_7$; (2) $D_6 \cap D_8$; (3) $D_3 \cup D_{12}$; (4) $D_3 \cap D_{12}$.

(*b*) Prove que $\cap(D_i: i \in J) = \varnothing$, onde J é um subconjunto infinito de $\mathbf{N}$.

Números Cardinais

3.41 Ache o número cardinal de cada conjunto:

(*a*) {domingo, segunda-feira, ..., sábado}

(*b*) $\{x: x$ é uma letra do alfabeto na palavra "BASEBALL"$\}$

(*c*) $\{x: x^2 = 9, 2x = 8\}$

(*d*) O conjunto Partes(A) onde $A = \{1, 5, 7, 11\}$

(*e*) Coleção das funções de $A = \{a, b, c\}$ em $B = \{1, 2, 3, 4\}$

(*f*) Conjunto das relações em $A = \{a, b, c\}$

3.42 Prove que:

(*a*) Todo conjunto infinito A tem um subconjunto enumerável D.

(*b*) Todo subconjunto de um conjunto enumerável é finito ou enumerável.

(*c*) Se A e B são enumeráveis, então $A \times B$ é enumerável.

(*d*) O conjunto $\mathbf{Q}$ dos números racionais é enumerável.

3.43 Prove que: (*a*) $|A \times B| = |B \times A|$. (*b*) Se $A \subseteq B$, então $|A| \leq |B|$. (*c*) Se $|A| = |B|$, então $|P(A)| = |P(B)|$.

3.44 Ache o número cardinal de cada conjunto: (*a*) a coleção X de funções de $A = \{a, b, c, d\}$ em $B = \{1, 2, 3, 4, 5\}$; (*b*) o conjunto Y de todas as relações em $A = \{a, b, c, d\}$.

Funções Especiais

3.45 Ache: (*a*) $\lfloor 13{,}2 \rfloor, \lfloor -0{,}17 \rfloor, \lfloor 34 \rfloor$; (*b*) $\lceil 13{,}2 \rceil, \lceil -0{,}17 \rceil, \lceil 34 \rceil$.

3.46 Ache: (*a*) $10 \pmod 3$; (*b*) $200 \pmod{20}$; (*c*) $5 \pmod{12}$; (*d*) $29 \pmod 6$; (*e*) $-347 \pmod 6$; (*f*) $-555 \pmod{11}$.

3.47 Ache: (*a*) $3! + 4!$; (*b*) $3!(3! + 2!)$; (*c*) $6!/5!$; (*d*) $30!/28!$.

3.48 Avalie (*a*) $\log_2 16$; (*b*) $\log_3 27$; (*c*) $\log_{10} 0{,}01$.

Problemas Variados

3.49 Prove: o conjunto P de todos os polinômios

$$p(x) = a_0 + a_1 x + \cdots + a_m x^m$$

com coeficientes inteiros, isto é, onde $a_0, a_1, \ldots, a_m$ são inteiros, é enumerável.

3.50 Sejam a e b inteiros e suponha que $Q(a, b)$ é definida recursivamente por:

$$Q(a,b) = \begin{cases} 5 & \text{se } a < b \\ Q(a-b,\ b+2) + a & \text{se } a \geq b \end{cases}$$

Ache $Q(2, 7)$, $Q(5, 3)$ e $Q(15, 2)$.

Respostas dos Problemas Complementares

3.29 (*a*) Não; (*b*) Sim; (*c*) Não.

3.30 (*a*) Sim; (*b*) Não; (*c*) Sim; (*d*) Não.

3.31 g = [(Carla, 4), (Marcos, 6), (Maria, 4), (Nina, 3), (Fabiana, 5)]

3.32 (*a*) $g = \{(1,2),(2,3),(3,1),(4,3)\}$; (*b*) $\{1,2,3\}$; (*c*) $g \circ g = \{(1,3),(2,1),(3,2),(4,1)\}$.

3.33 (*a*) $\{(1,1),(2,4),(3,3),(4,3)$. (*b*) $\{(1,1),(2,2),(3,1),(4,1)$. (*c*) $\{(1,4),(2,3),(3,3),(4,4)$.

3.34 $f^{-1}(x) = \dfrac{x+7}{3}$

3.38 (*a*) A_5; (*b*) A_7; (*c*) A_r, onde r é o menor inteiro em J; (*d*) A_s, onde s é o maior inteiro em J; (*e*) A_r, on
de r é o menor inteiro em K; (*f*) $\varnothing$.

3.40 (1) D_{14}; (2) D_{24}; (3) D_3; (4) D_{12}.

3.41 (*a*) 7; (*b*) 5; (*c*) 0; (*d*) 16; (*e*) $4^3 = 64$; (*f*) $2^9 = 512$.

3.44 (*a*) $5^4 - 625$; (*b*) $2^{16} = 65.536$.

3.45 (*a*) 13, −1, 34; (*b*) 14, 0, 34.

3.46 (*a*) 1; (*b*) 0; (*c*) 2; (*d*) 5; (*e*) $6 - 5 = 1$; (*f*) $11 - 5 = 6$.

3.47 (*a*) 30; (*b*) 48; (*c*) 6; (*d*) 870.

3.48 (*a*) 4; (*b*) 3; (*c*) −2.

3.49 *Sugestão*: seja P_k o conjunto de todos os polinômios $P(x)$ tais que $m \leq k$ e cada $|a_i| \leq m$. Então, P_k é finito e $P = \cup_k P_k$

3.50 $Q(2, 7) = 5$, $Q(5, 3) = 10$, $Q(15, 2) = 42$.

Capítulo 4

Lógica e Cálculo Proposicional

4.1 INTRODUÇÃO

Muitas demonstrações em matemática e muitos algoritmos em ciência da computação usam expressões lógicas tais como

"SE p ENTÃO q" ou "SE p_1 E p_2, ENTÃO q_1 OU q_2"

É, portanto, necessário conhecer os casos nos quais essas expressões têm valor FALSO ou VERDADEIRO, o que denominamos valor lógico de tais expressões. Discutimos essas questões nesta seção.

Também investigamos o valor lógico de declarações com quantificadores, que são aquelas que usam os quantificadores lógicos "para todo" e "existe".

4.2 PROPOSIÇÕES E PROPOSIÇÕES COMPOSTAS

Uma *proposição* (ou *declaração*) é uma sentença declarativa que pode ser verdadeira ou falsa, mas não ambos. Considere, por exemplo, as seguintes oito sentenças:

(i) Paris fica na França.

(ii) $1 + 1 = 2$.

(iii) $2 + 2 = 3$.

(iv) Londres fica na Dinamarca.

(v) $9 < 6$.

(vi) $x = 2$ é solução de $x^2 = 4$.

(vii) Aonde você está indo?

(viii) Faça seu dever de casa.

Todas elas, exceto (vii) e (viii), são proposições. Ademais, (i), (ii) e (vi) são verdadeiras, enquanto (iii), (iv) e (v) são falsas.

Proposições Compostas

Muitas proposições são *compostas*, isto é, formadas de *subproposições* e vários conectivos, discutidos subseqüentemente. Estas proposições são chamadas *proposições compostas*. Uma proposição é dita *primitiva* se não pode ser subdividida em duas proposições mais simples, isto é, se não é composta.

Exemplo 4.1

(*a*) "Rosas são vermelhas e violetas são azuis" é uma proposição composta com as subproposições "rosas são vermelhas" e "violetas são azuis".

(*b*) "João é inteligente ou estuda toda noite" é uma proposição composta com as subproposições "João é inteligente" e "João estuda toda noite".

(*c*) As proposições (i) a (vi) anteriores são proposições primitivas; não podem ser subdivididas em proposições mais simples.

A propriedade fundamental de uma proposição composta é que seu valor lógico fica completamente determinado pelo valor lógico das suas subproposições juntamente com o modo pelo qual essas subproposições estão conectadas para formar a proposição composta. A próxima seção estuda alguns desses conectivos.

4.3 OPERAÇÕES LÓGICAS BÁSICAS

Esta seção estuda as três operações lógicas básicas de conjunção, disjunção e negação, que correspondem, respectivamente, às palavras "e", "ou" e "não".

Conjunção: $p \wedge q$

Quaisquer duas proposições podem ser combinadas pela palavra "e" para formar uma composição composta chamada de *conjunção* das proposições originais. Simbolicamente,

$$p \wedge q$$

(lê-se "p e q") denota a conjunção de p e q. Como $p \wedge q$ é uma proposição, tem um valor lógico que depende apenas dos valores lógicos de p e q.

Definição 4-1: se p e q são verdadeiras, então $p \wedge q$ é verdadeira; caso contrário, $p \wedge q$ é falsa.

O valor lógico de $p \wedge q$ pode ser definido equivalentemente pela tabela na Figura 4-1(*a*). Na tabela, a primeira linha contém uma maneira sucinta de dizer que, se p é verdade e q é verdade, então $p \wedge q$ é verdade. A segunda linha diz que, se p é verdade e q é falso, então $p \wedge q$ é falso, e assim por diante. Observe que existem quatro linhas correspondentes às quatro possíveis combinações de V ou F para as duas subproposições p e q. Note que $p \wedge q$ é verdade apenas quando p e q são verdade.

Exemplo 4.2 Considere as quatro declarações seguintes:

(i) Paris fica na França e $2 + 2 = 4$.

(ii) Paris fica na França e $2 + 2 = 5$.

(iii) Paris fica na Inglaterra e $2 + 2 = 4$.

(iv) Paris fica na Inglaterra e $2 + 2 = 5$.

Apenas a primeira declaração é verdade. Cada uma das outras declarações é falsa, já que pelo menos uma das suas subdeclarações é falsa.

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

(*a*) "p e q"

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

(*b*) "p ou q"

p	$\neg p$
V	F
F	V

(*c*) "não p"

Fig. 4-1

Disjunção: $p \vee q$

Quaisquer duas proposições podem ser combinadas pela palavra "ou" para formar uma proposição composta chamada *disjunção* das proposições originais. Simbolicamente,

$$p \vee q$$

(lê-se "p ou q") denota a disjunção de p e q. O valor lógico de $p \vee q$ depende apenas dos valores de p e q como descrito a seguir.

Definição 4.2: Se p e q são falsas, então $p \vee q$ é falsa; caso contrário, $p \vee q$ é verdade.

O valor lógico de p ou q pode ser equivalentemente definido pela Tabela 4-1(b). Observe que $p \vee q$ é falsa apenas no quarto caso, quando ambas, p e q, são falsas.

Exemplo 4.3 Considere as seguintes quatro afirmações:

(i) Paris fica na França e $2 + 2 = 4$.
(ii) Paris fica na França e $2 + 2 = 5$.
(iii) Paris fica na Inglaterra e $2 + 2 = 4$.
(iv) Paris fica na Inglaterra e $2 + 2 = 5$.

Apenas a última declaração (iv) é falsa. Cada uma das outras declarações é verdade, já que pelo menos uma das suas subdeclarações é verdade.

Observação: A palavra "ou" é normalmente usada de duas maneiras distintas. Às vezes é usada com o sentido de "p ou q ou ambas", i.e., pelo menos uma das duas alternativas ocorre, como acima, e outras vezes tem o significado de "p ou q, mas não ambas", i.e., pelo menos uma das duas alternativas ocorre. Por exemplo, a sentença "ele irá para Harvard ou Yale" utiliza "ou" da segunda forma, conhecida como *disjunção exclusiva*. A menos que se explicite o contrário, "ou" será utilizado com o primeiro sentido. Essa discussão realça a precisão obtida pelo uso da linguagem simbólica: $p \vee q$ é definida pela sua tabela-verdade e sempre tem o significado de "p e/ou q".

Negação: $\neg p$

Dada qualquer proposição p, outra proposição, denominada *negação* de p, pode ser formada escrevendo "não ocorre que…" ou "é falso que…" antes de p, ou, se possível, inserindo em p a palavra "não". Simbolicamente,

$$\neg p$$

(lê-se "não p") denota a negação de p. O valor lógico de $\neg p$ depende do valor lógico de p como a seguir.

Definição 4.3: Se p é verdade, então $\neg p$ é falso; se p é falso então $\neg p$ é verdade.

O valor lógico de $\neg p$ pode ser definido equivalentemente pela tabela na Figura 4-1(c). O valor lógico da negação de p é sempre o oposto do valor lógico de p.

Exemplo 4.4 Considere as seis declarações seguintes:

(a_1) Paris fica na França.
(a_2) Não ocorre que Paris fique na França.
(a_3) Paris não fica na França.
(b_1) $2 + 2 = 5$.
(b_2) Não ocorre que $2 + 2 = 5$.
(b_3) $2 + 2 \neq 5$.

Então, (a_2) e (a_3) são a negação de (a_1); e (b_2) e (b_3) são a negação de (b_1). Como (a_1) é verdade, (a_2) e (a_3) são falsas; e como (b_1) é falsa, (b_2) e (b_3) são verdade.

Observação: A notação lógica para os conectivos "e", "ou" e "não" não é completamente padronizada. Por exemplo, alguns textos usam:

$p \,\&\, q$, $p \cdot q$ ou pq	para $p \wedge q$
$p + q$	para $p \vee q$
p', $\bar{p}$ ou $\sim p$	para $\neg p$

4.4 PROPOSIÇÕES E TABELAS-VERDADE

Seja $P(p,q,\ldots)$ a expressão construída a partir das variáveis lógicas p, q,... que assumem valores VERDADEIRO (V) ou FALSO (F), e os conectivos lógicos, $\wedge$, $\vee$ e $\neg$ (e outros, discutidos posteriormente). Uma tal expressão $P(p, q,\ldots)$ será denominada uma *proposição*.

A propriedade principal de uma proposição $P(p, q,\ldots)$ é o seu valor lógico depender exclusivamente dos valores lógicos das sua variáveis, isto é, o valor lógico de uma proposição é conhecido se os valores lógicos de suas variáveis são conhecidos. Uma maneira concisa de ilustrar essa relação é pela *tabela-verdade*. Descrevemos uma forma de obter uma tabela-verdade abaixo.

Considere, por exemplo, a proposição $\neg (p \wedge \neg q)$. A Figura 4-2(a) indica como a tabela-verdade de $\neg (p \wedge q)$ é construída. Observe que as primeiras coluna da tabela são para as variáveis p, q,... e que existem linhas suficientes na tabela para todas as combinações possíveis de V ou F para estas *variáveis*. (Para duas variáveis, como acima, quatro linhas são necessárias; para três variáveis, oito linhas são necessárias; e, em geral, para n variáveis, 2^n linhas são usadas.) Existe então uma coluna para cada fase "elementar" da construção da proposição, sendo o valor lógico, a cada passo, determinado a partir das fases anteriores usando a definição dos conectivos $\wedge$, $\vee$, $\neg$. Finalmente obtemos o valor lógico da proposição, que aparece na última coluna.

A tabela-verdade da proposição $\neg (p \wedge \neg q)$ é mostrada na Figura 4-2(b). Ela consiste precisamente nas colunas da Figura 4-2(a) que aparecem abaixo das variáveis e da proposição; as outras colunas são usadas meramente na construção da tabela-verdade.

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
V	V	F	F	V
V	F	V	V	F
F	V	F	F	V
F	F	V	F	V

(a)

p	q	$\neg(p \wedge \neg q)$
V	V	V
V	F	F
F	V	V
F	F	V

(b)

Fig. 4-2

Observação: A fim de evitar um número excessivo de parênteses, às vezes adotamos uma ordem de precedência para os conectivos lógicos. Especificamente,

$\neg$ tem precedência sobre $\wedge$ que tem precedência sobre $\vee$.

Por exemplo, $\neg p \wedge q$ significa $(\neg p) \wedge q$, e não $\neg (p \wedge q)$.

Método Alternativo para Construir uma Tabela-Verdade

Uma outra maneira de construir uma tabela-verdade para $\neg (p \wedge \neg q)$ é a seguinte:

(a) Primeiramente construa a tabela-verdade mostrada na Figura 4-3. Isto é, primeiramente listamos todas as variáveis e as combinações dos seus valores lógicos. Então a proposição é escrita na linha superior, à direita das suas variáveis com espaço suficiente para existir uma coluna abaixo de cada variável e de cada conectivo na proposição. Há ainda uma linha final denominada "Passos".

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V					
V	F					
F	V					
F	F					
Passos						

Fig. 4-3

(b) A seguir, valores lógicos adicionais são colocados na tabela-verdade em várias etapas, como mostrado na Figura 4-4. Isto é, primeiramente os valores lógicos das variáveis são colocados abaixo delas na proposição e, então, há uma coluna de valores lógicos colocada abaixo de cada operação lógica. Indicamos também o passo em que cada coluna de valores lógicos é colocada na tabela.

A tabela-verdade da proposição então consiste nas colunas originais sob as variáveis e no último passo, isto é, a última coluna colocada na tabela.

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V			V
V	F		V			F
F	V		F			V
F	F		F			F
Passos			1			1

(*a*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V		F	V
V	F		V		V	F
F	V		F		F	V
F	F		F		V	F
Passos			1		2	1

(*b*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V		V	F	F	V
V	F		V	V	V	F
F	V		F	F	F	V
F	F		F	F	V	F
Passos			1	3	2	1

(*c*)

p	q	$\neg$	$(p$	$\wedge$	$\neg$	$q)$
V	V	V	V	F	F	V
V	V	F	V	V	V	F
F	F	V	F	F	F	V
F	F	V	F	F	V	F
Passos		4	1	3	2	1

(*d*)

Fig. 4-4

4.5 TAUTOLOGIAS E CONTRADIÇÕES

Algumas proposições $P(p, q,\ldots)$ contêm apenas V na última coluna das suas tabelas-verdade, ou, em outras palavras, elas são verdade para quaisquer valores lógicos das sua variáveis. Tais proposições são chamadas tautologias. Analogamente, $P(p, q,\ldots)$ é dita uma contradição se contiver apenas F na última coluna da sua tabela-verdade, ou, em outras palavras, é falsa para quaisquer valores lógicos das suas variáveis. Por exemplo, a proposição "p ou não p", isto é, $p \vee \neg p$, é uma tautologia, e a proposição "p e não p", isto é, $p \wedge \neg p$, é uma contradição. Esse fato pode ser verificado analisando suas tabelas-verdade na Figura 4-5 (as tabelas-verdade têm apenas duas linhas, já que cada proposição tem apenas uma variável).

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

(*a*) $p \vee \neg p$

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

(*b*) $p \wedge \neg p$

Fig. 4-5

Note que a negação de uma tautologia é uma contradição, já que é sempre falsa, e a negação de uma contradição é uma tautologia, já que é sempre verdadeira.

Seja $P(p, q,\ldots)$ uma tautologia, e sejam $P_1(p, q,\ldots)$, $P_2(p, q,\ldots)$, ... proposições quaisquer. Como $P(p, q,\ldots)$ não depende dos valores lógicos de suas variáveis $p, q,\ldots$, podemos substituir P_1 por p, P_2 por $q,\ldots$ na tautologia $P(p, q,\ldots)$ e ainda ter uma tautologia. Em outras palavras:

Teorema 4-1: **(Princípio da substituição)** se $P(p, q,\ldots)$ é uma tautologia, então $P(P_1, P_2,\ldots)$ é uma tautologia para quaisquer proposições.

4.6 EQUIVALÊNCIA LÓGICA

Duas proposições $P(p, q,\ldots)$ e $Q(p, q,\ldots)$ são ditas *logicamente equivalentes* ou, simplesmente, *equivalentes* ou *iguais*, denotando-se por

$$P(p, q, \ldots) \equiv Q(p, q, \ldots)$$

se elas têm tabelas-verdade idênticas. Considere, por exemplo, as tabelas-verdade de $\neg (p \wedge q)$ e $\neg p \vee \neg q$ que aparecem na Figura 4-6. Observe que as duas são iguais, isto é, ambas as proposições são falsas no primeiro caso e verdadeiras nos outros três. Conseqüentemente, podemos escrever

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

Em outras palavras, as proposições são logicamente equivalentes.

Observação: Considere a declaração:

"Não é verdade que rosas são vermelhas e violetas são azuis"

Essa declaração pode ser escrita na forma $\neg (p \vee q)$, onde

p é "rosas são vermelhas" e q é "violetas são azuis"

Entretanto, como observado acima, $\neg (p \wedge q) \equiv \neg p \vee \neg q$. Por conseguinte, a declaração

"Rosas não são vermelhas ou violetas não são azuis"

tem o mesmo significado que a declaração dada.

p	q	$p \wedge q$	$\neg (p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

(a) $\neg (p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

(b) $\neg p \vee \neg q$

Fig. 4-6

4.7 ÁLGEBRA DAS PROPOSIÇÕES

As proposições satisfazem várias leis que estão listadas na Tabela 4-1. (Nessa tabela, V e F significam os valores lógicos "verdadeiro" e "falso", respectivamente.) Apresentamos esse resultado formalmente.

Teorema 4-2: as proposições satisfazem as leis da Tabela 4-1.

Tabela 4-1 Leis da álgebra das proposições

Leis de idempotência	
(1a) $p \vee p \equiv p$	(1b) $p \wedge p \equiv p$
Leis de associatividade	
(2a) $(p \vee q) \vee r \equiv p \vee (q \vee r)$	(2b) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Leis de comutatividade	
(3a) $p \vee q \equiv q \vee p$	(3b) $p \wedge q \equiv q \wedge p$
Leis de distributividade	
(4a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	(4b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Leis de identidade	
(5a) $p \vee \mathrm{F} \equiv p$	(5b) $p \wedge \mathrm{V} \equiv p$
(6a) $p \vee \mathrm{V} \equiv \mathrm{V}$	(6b) $p \wedge \mathrm{F} \equiv \mathrm{F}$
Leis dos complementares	
(7a) $p \vee \neg p \equiv \mathrm{V}$	(7b) $p \wedge \neg p \equiv \mathrm{F}$
(8a) $\neg \mathrm{V} \equiv \mathrm{F}$	(8b) $\neg \mathrm{F} \equiv \mathrm{V}$
Leis de involução	
(9) $\neg \neg p \equiv p$	
Leis de DeMorgan	
(10a) $\neg (p \vee q) \equiv \neg p \wedge \neg q$	(10b) $\neg (p \wedge q) \equiv \neg p \vee \neg q$

4.8 DECLARAÇÕES CONDICIONAIS E BICONDICIONAIS

Muitas declarações, particularmente em matemática, são da forma "se p então q". Tais declarações são chamadas de *condicionais* e denotadas por

$$p \to q$$

A declaração $p \to q$ é freqüentemente lida como "p implica q" ou "p apenas se q".

Uma outra declaração comum é da forma "p se e somente se q". Esse tipo de declaração é denominado *bicondicional* e é denotado por

$$p \leftrightarrow q$$

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

(*a*) $p \to q$

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

(*b*) $p \leftrightarrow q$

Fig. 4-7

p	q	$\neg p$	$\neg p \vee q$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

$\neg p \vee q$

Fig. 4-8

Os valores lógicos de $p \to q$ e $p \leftrightarrow q$ são definidos pelas tabelas na Figura 4-7. Observe que:

(*a*) A condicional $p \to q$ é falsa apenas quando a primeira parte p é verdadeira e a segunda parte p é falsa. Conseqüentemente, quando p é falsa, a condicional $p \to q$ é verdadeira, não importando o valor lógico de q.

(*b*) A bicondicional $p \leftrightarrow q$ é verdadeira sempre que p e q têm os mesmos valores lógicos, e falsa caso contrário.

A tabela-verdade da proposição $\neg p \vee q$ aparece na Figura 4-8. Observe que as tabelas-verdade de $\neg p \vee q$ e $p \to q$ são idênticas, isto é, são ambas falsas apenas no segundo caso. Conseqüentemente, $p \to q$ é logicamente equivalente a $\neg p \vee q$; isto é,

$$p \to q \equiv \neg p \vee q$$

Em outras palavras, a declaração condicional "Se p então q" é logicamente equivalente à declaração "não p ou q", que envolve apenas os conectivos $\vee$ e $\neg$, e, portanto, já era parte da nossa linguagem. Podemos considerar $p \to q$ como uma abreviação para uma declaração que já pertencia à linguagem.

4.9 ARGUMENTOS

Um *argumento* é uma afirmação de que um dado conjunto de proposições $P_1, P_2, \ldots, P_n$, chamadas de *premissas*[†], conduz (tem como conseqüência) a uma outra proposição Q, chamada de *conclusão*. Tal argumento é denotado por

$$P_1, P_2, \ldots, P_n \vdash Q$$

A noção de um "argumento lógico" ou "argumento válido" é formalizada como a seguir:

Definição 4.4: Um argumento $P_1, P_2, \ldots, P_n \vdash Q$ é dito *válido* se Q for verdade sempre que todas as premissas $P_1, P_2, \ldots, P_n$ são verdade.

Um argumento que não é válido é dito uma *falácia*.

Exemplo 4.5

(*a*) O seguinte argumento é válido:

$$p, p \to q \vdash q \quad (\textbf{\textit{Modus Ponens}})$$

A demonstração desta regra segue da tabela-verdade na Figura 4-9. Especificamente, p e $p \to q$ são simultaneamente verdade apenas no Caso (linha) 1, e neste caso q é verdade.

[†] N. de T. No original, *premises*; em português, freqüentemente também se usa o termo "hipótese".

(*b*) O seguinte argumento é uma falácia:

$$p \to q, q \vdash p$$

Pois $p \to q$ e q são ambos verdade no Caso (linha) 3 da tabela-verdade na Figura 4-9, mas, neste caso, p é falso.

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

Fig. 4-9

As proposições $P_1, P_2, \ldots, P_n$ são simultaneamente verdadeiras se e somente se a proposição $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ é verdadeira. O argumento $P_1, P_2, \ldots, P_n \vdash Q$ é válido se e somente se Q é verdade sempre que $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ é verdade ou, equivalentemente, se a proposição $(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \to Q$ é uma tautologia. Afirmamos esse resultado formalmente.

Teorema 4-3: O argumento $P_1, P_2, \ldots, P_n \vdash Q$ é valido se e somente se a proposição $(P_1 \wedge P_2 \ldots \wedge P_n) \to Q$ é uma tautologia.

Aplicamos esse teorema no próximo exemplo.

Exemplo 4.6 Um princípio fundamental de argumentos lógicos:

"Se p implica q e q implica r, então p implica r."

Isto é, o seguinte argumento é válido:

$$p \to q, q \to r \vdash p \to r \quad (\textit{Lei do silogismo})$$

Este fato é verificado pela tabela-verdade na Figura 4-10, que mostra que a seguinte proposição é uma tautologia:

$$[(p \to q) \wedge (q \to r)] \to (p \to r)$$

Equivalentemente, o argumento é válido uma vez que as premissas $p \to q$ e $q \to r$ são simultaneamente verdadeiras apenas nos Casos (linhas)1, 5, 7 e 8 e, nestes casos, a conclusão $p \to r$ também é verdade. (Observe que a tabela-verdade requer $2^3 = 8$ linhas, já que existem três variáveis, p, q e r.)

p	q	r	$[(p$	$\to$	$q)$	$\wedge$	$(q$	$\to$	$r)]$	$\to$	$(p$	$\to$	$r)$
V	V	V	V	V	V	V	V	V	V	V	V	V	V
V	V	F	V	V	V	F	V	F	F	V	V	F	F
V	F	V	V	F	F	F	F	V	V	V	V	V	V
V	F	F	V	F	F	F	F	V	F	V	V	F	F
F	V	V	F	V	V	V	V	V	V	V	F	V	V
F	V	F	F	V	V	F	V	F	F	V	F	V	F
F	F	V	F	V	F	V	F	V	V	V	F	V	V
F	F	F	F	V	F	V	F	V	F	V	F	V	F
Passos			1	2	1	3	1	2	1	4	1	2	1

Fig. 4-2

Aplicamos agora a teoria acima a argumentos envolvendo declarações específicas. Enfatizamos que a validade de um argumento não depende dos valores lógicos nem do conteúdo das declarações usadas no argumento, mas da forma particular do argumento. Esse fato está ilustrado no exemplo seguinte.

Exemplo 4.7 Considere o seguinte argumento:

S_1: Se um homem é solteiro, é infeliz.
S_2: Se um homem é infeliz, morre jovem.

S: Solteiros morrem jovens.

Aqui, a afirmação S abaixo da linha denota a conclusão do argumento, e as afirmações S_1 e S_2 acima da linha denotam as premissas. Afirmamos que o argumento $S_1, S_2 \vdash S$ é válido, pois o argumento é da forma

$$p \to q, q \to r \vdash p \to r$$

onde p é "Ele é um solteiro", q é "Ele é infeliz" e r é "Ele morre jovem"; e pelo Exemplo 4.6, este argumento (lei do silogismo) é válido.

4.10 IMPLICAÇÃO LÓGICA

Diz-se que uma proposição $P(p, q,\ldots)$ *implica logicamente* uma proposição $Q(p, q,\ldots)$, escrevendo

$$P(p, q, \ldots) \Rightarrow Q(p, q, \ldots)$$

se $Q(p, q,\ldots)$ é verdade sempre que $P(p, q,\ldots)$ é verdade.

Exemplo 4.8 Afirmamos que p implica logicamente $p \vee q$. Considere a tabela-verdade na Figura 4-11. Observe que p é verdade nos Casos (linhas) 1 e 2, e nestes casos $p \vee q$ também é verdade. Logo, $p \Rightarrow p \vee q$.

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Fig. 4-11

Agora, se $Q(p, q,\ldots)$ é verdade sempre que $P(p, q,\ldots)$ for verdade, então o argumento

$$P(p, q, \ldots) \vdash Q(p, q, \ldots)$$

é válido; e a recíproca é verdadeira. Ademais, o argumento $P \vdash Q$ é válido se e somente se a declaração condicional $P \to Q$ é sempre verdade, i. e., uma tautologia. Afirmamos esse resultado formalmente.

Teorema 4-4: Para quaisquer proposições $P(p, q,\ldots)$ e $Q(p, q,\ldots)$, as três afirmações seguintes são equivalentes:

(i) $P(p, q,\ldots)$ implica logicamente $Q(p, q,\ldots)$.
(ii) O argumento $P(p, q, \ldots) \vdash Q(p, q, \ldots)$ é válido.
(iii) A proposição $P(p, q,\ldots) \to Q(p, q,\ldots)$ é uma tautologia.

Notamos que alguns autores da área de lógica formal e muitos textos usam o termo "implica" com o mesmo sentido que usamos "implica logicamente", e, portanto, distinguem "implica" de "se … então". Esses dois conceitos são, obviamente, intimamente relacionados como visto no teorema acima.

4.11 FUNÇÕES PROPOSICIONAIS E QUANTIFICADORES

Seja A um conjunto dado. Uma *função proposicional* (ou uma *sentença aberta* ou *condição*) definida em A é uma expressão:

$$p(x)$$

que tem a propriedade que $p(a)$ é verdadeira ou falsa para cada $a \in A$. Isto é, $p(x)$ se torna uma declaração (munida de um valor lógico) sempre que algum elemento $a \in A$ é substituído pela variável x. O conjunto A é dito o domínio de $p(x)$, e o conjunto T_p de todos os elementos de A para os quais $p(a)$ é verdadeira é chamado *conjunto verdade* de $p(x)$. Em outras palavras,

$$T_p = \{x: x \in A,\ p(x) \text{ é verdade}\} \quad \text{ou} \quad T_p = \{x: p(x)\}$$

Freqüentemente, quando A é um conjunto de números, a condição $p(x)$ tem a forma de uma equação ou desigualdade envolvendo a variável x.

Exemplo 4.9 Ache o conjunto verdade de cada função proposicional $p(x)$ definida no conjunto **N** dos inteiros positivos.

(*a*) Seja $p(x)$ "$x + 2 > 7$". O conjunto verdade é

$$\{x: x \in \mathbf{N},\ x + 2 > 7\} = \{6, 7, 8, \ldots\}$$

consistindo em todos os inteiros maiores do que 5.

(*b*) Seja $p(x)$ "$x + 5 < 3$". O conjunto verdade é

$$\{x: x \in \mathbf{N},\ x + 5 < 3\} = \varnothing$$

o conjunto vazio. Em outras palavras, $p(x)$ não é verdade para nenhum inteiro positivo em **N**.

(*c*) Seja $p(x)$ "$x + 5 > 1$". O conjunto verdade é

$$\{x: x \in \mathbf{N},\ x + 5 > 1\} = \mathbf{N}$$

Portanto, $p(x)$ é verdade para todo elemento em **N**.

Observação: O exemplo acima mostra que, se $p(x)$ é uma função proposicional definida em um conjunto A, então $p(x)$ pode ser verdade para todo $x \in A$, para algum $x \in A$, ou para nenhum $x \in A$. As duas próximas subseções discutem quantificadores relacionados com essas funções proposicionais.

Quantificador Universal

Seja $p(x)$ um função proposicional definida em um conjunto A. Considere as expressões

$$(\forall x \in A)p(x) \qquad \text{e} \qquad \forall x\ p(x) \tag{4.1}$$

lidas como "Para todo x em A, $p(x)$ é uma declaração verdadeira" ou, simplesmente, "Para todo x, $p(x)$ ". O símbolo

$$\forall$$

que se lê "para todo" é dito *quantificador universal*. A declaração (*4.1*) é equivalente à declaração

$$T_p = \{x: x \in A,\ p(x)\} = A \tag{4.2}$$

isto é, o conjunto verdade de $p(x)$ é todo o conjunto A.

A expressão $p(x)$, por si só, é uma sentença aberta ou condição e, portanto, não tem valor lógico. Entretanto, $\forall x\ p(x)$, isto é, $p(x)$ precedido pelo quantificador universal $\forall$, tem um valor lógico que segue de (*4.1*) e (*4.2*). Especificamente,

Q_1: se $\{x: x \in A, p(x)\} = A$, então $\forall x\ p(x)$ é verdade; caso contrário, $\forall x\ p(x)$ é falsa.

Exemplo 4.10

(*a*) A proposição $(\forall n \in \mathbf{N})(n + 4 > 3)$ é verdade, já que

$$\{n: n + 4 > 3\} = \{1, 2, 3, \ldots\} = \mathbf{N}$$

(*b*) A proposição $(\forall n \in \mathbf{N})(n + 2 > 8)$ é falsa, já que

$$\{n: n + 2 > 8\} = \{7, 8, \ldots\} \neq \mathbf{N}$$

(*c*) O símbolo $\forall$ pode ser usado para definir a interseção de uma coleção indexada de conjuntos $\{A_i: i \in I\}$ como a seguir:

$$\cap(A_i: i \in I) = \{x: \forall_i \in I,\ x \in A_i\}$$

Quantificador Existencial

Seja $p(x)$ uma função proposicional definida em um conjunto A. Considere a expressão:

$$(\exists x \in A)p(x) \qquad \text{ou} \qquad \exists x,\ p(x) \tag{4.3}$$

que se lê "Existe um x em A tal que $p(x)$ é uma declaração verdadeira" ou, simplesmente, "Para algum x, $p(x)$ ". O símbolo

$$\exists$$

que se lê "existe" ou "para algum" ou "para pelo menos um" é chamado de *quantificador existencial*. A declaração (*4.3*) é equivalente à declaração

$$T_p = \{x: x \in A,\ p(x)\} \neq \varnothing \tag{4.4}$$

i.e., o conjunto verdade de $p(x)$ não é vazio. Conseqüentemente, $\exists\, x\, p(x)$, isto é, $p(x)$ precedido pelo quantificador $\exists$, tem um valor lógico. Especificamente:

Q_2: se $\{x: p(x)\} \neq \varnothing$, então $\exists\, x\ p(x)$ é verdade; caso contrário, $\exists x\, p(x)$ é falsa.

Exemplo 4.11

(*a*) A proposição $(\exists n \in \mathbf{N})(n + 4 < 7)$ é verdade, já que $\{n: n + 4 < 7\} = \{1, 2\} \neq \varnothing$.

(*b*) A proposição $(\exists n \in \mathbf{N})(n + 6 < 4)$ é falsa, já que $\{n: n + 6 < 4\} = \varnothing$.

(*c*) O símbolo $\exists$ pode ser usado para definir a união de coleções indexadas $\{A_i: i \in I\}$ de conjuntos A_i como a seguir:

$$\cup(A_i: i \in I) = \{x: \exists i \in I,\ x \in A_i\}$$

Notação

Seja $A = \{2, 3, 5\}$, e seja $p(x)$ a sentença "x é um número primo" ou, simplesmente, "x é primo". Então,

"Dois é primo e três é primo e cinco é primo" $\qquad (*)$

pode ser denotada por

$$p(2) \wedge p(3) \wedge p(5) \qquad \text{ou} \qquad \wedge\,(a \in A,\ p(a))$$

que é equivalente à declaração

"Todo número em A é primo" $\qquad$ ou $\qquad \forall a \in A,\ p(a) \qquad (**)$

Analogamente, a proposição

"Dois é primo ou três é primo ou cinco é primo"

pode ser denotada por

$$p(2) \vee p(3) \vee p(5) \qquad \text{ou} \qquad \vee\,(a \in A,\ p(a))$$

que é equivalente à declaração

"Pelo menos um número em A é primo" $\qquad$ ou $\qquad \exists\, a \in A,\ p(a)$

Em outras palavras,

$$\wedge(a \in A,\ p(a)) \equiv \forall a \in A,\ p(a) \qquad \text{e} \qquad \vee\,(a \in A,\ p(a)) \equiv \exists a \in A,\ p(a)$$

Portanto, os símbolos $\wedge$ e $\vee$ são, às vezes, usados no lugar de $\forall$ e $\exists$.

Observação: Se A é um conjunto infinito, então uma declaração da forma $(*)$ não pode ser feita, uma vez que a sentença não terminará; porém, uma declaração da forma $(**)$ sempre pode ser feita, mesmo quando A é infinito.

4.12 NEGAÇÃO DE DECLARAÇÕES COM QUANTIFICADORES

Considere a declaração: "Todos os grandes matemáticos são do sexo masculino". Sua negativa é:

"Não ocorre que todos os grandes matemáticos são do sexo masculino" ou, equivalentemente,

"Existe pelo menos um grande matemático que é do sexo feminino (não masculino)"

Em símbolos, usando $\boldsymbol{M}$ para denotar o conjunto de grandes matemáticos, as expressões acima podem ser escritas como

$$\neg(\forall x \in M)\,(x \text{ é masculino}) \equiv (\exists\, x \in M)\ (x \text{ não é masculino})$$

ou, onde $p(x)$ denota "x é do sexo masculino",

$$\neg(\forall x \in M)p(x) \equiv (\exists\, x \in M)\neg\, p(x) \qquad \text{ou} \qquad \neg\forall x p(x) \equiv \exists\, x \neg\, p(x)$$

O enunciado acima é verdade para qualquer proposição $p(x)$. Isto é,

***Teorema 4-5* (DeMorgan):** $\neg\,(\forall x \in A)p(x) \equiv (\exists\, x \in A)\neg\, p(x)$.

Em outras palavras, as duas declarações seguintes são equivalentes:

(1) Não é verdade que, para todo $a \in A$, $p(a)$ é verdade.

(2) Existe um $a \in A$ tal que $p(a)$ é falsa.

Existe um teorema análogo para a negação de uma proposição que contém o quantificador existencial.

***Teorema 4-6* (DeMorgan):** $\neg\,(\exists x \in A)p(x) \equiv (\forall x \in A)\neg\, p(x)$.

Isto é, as duas declarações seguintes são equivalentes:

(1) Não é verdade que, para algum $a \in A$, $p(a)$ seja verdade.

(2) Para todo $a \in A$, $p(a)$ é falsa.

Exemplo 4.12

(*a*) As seguintes declarações são as negativas uma da outra:

"Para todos os inteiros positivos n, temos $n + 2 > 8$."
"Existe um inteiro positivo n, tal que $n + 2 \geqslant 8$."

(*b*) As seguintes declarações também são as negativas uma da outra:

"Existe uma pessoa (viva) com 150 anos."
"Toda pessoa viva não tem 150 anos."

Observação: A expressão $\neg\, p(x)$ tem o significado óbvio, a saber:

"A declaração $\neg\, p(a)$ é verdade quando $p(a)$ é falsa e vice-versa."

Anteriormente, $\neg$ foi usado como uma operação em declarações; aqui, $\neg$ é usado como uma operação em funções proposicionais. De maneira similar, $p(x) \wedge q(x)$, lido "$p(x)$ e $q(x)$", é definido por:

"A declaração $p(a) \wedge q(a)$ é verdade quando $p(a)$ e $q(a)$ são verdade."

De maneira similar, $p(x) \vee q(x)$, lido "$p(x)$ ou $q(x)$", é definido por:

"A declaração $p(a) \vee q(a)$ é verdade quando $p(a)$ ou $q(a)$ é verdade."

Portanto, em termos de conjunto verdade:

(i) $\neg\, p(x)$ é o complemento de $p(x)$.

(ii) $p(x) \wedge q(x)$ é a interseção de $p(x)$ e $q(x)$.

(iii) $p(x) \vee q(x)$ é a união de $p(x)$ e $q(x)$.

Também se pode mostrar que as leis para proposições se aplicam para funções proposicionais. Como exemplo, temos as leis de DeMorgan;

$$\neg (p(x) \wedge q(x)) \equiv \neg p(x) \vee \neg q(x) \qquad \text{e} \qquad \neg (p(x) \vee q(x)) \equiv \neg p(x) \wedge \neg q(x)$$

Contra-exemplo

O Teorema 4.6 diz que mostrar que uma declaração $\forall x, p(x)$ é falsa é equivalente a mostrar que $\exists\, x \neg p(x)$ é verdade ou, em outras palavras, que existe um elemento x_0 com a propriedade de que $p(x_0)$ é falsa. Tal elemento x_0 é dito um *contra-exemplo* para a declaração $\forall x, p(x)$.

Exemplo 4.13

(*a*) Considere a declaração $\forall\, x \in \mathbf{R}, |x| \neq 0$. A declaração é falsa uma vez que 0 é um contra-exemplo, isto é, $|0| \neq 0$ não é verdade.

(*b*) Considere a declaração $\forall x \in \mathbf{R},\ x^2 > x$. A declaração não é verdade uma vez que, por exemplo, $\frac{1}{2}$ é um contra-exemplo. Especificamente, $(\frac{1}{2})^2 \geq \frac{1}{2}$ não é verdade, isto é, $(\frac{1}{2})^2 < \frac{1}{2}$.

(*c*) Considere a declaração $\forall x \in \mathbf{N},\ x^2 \geq x$. Essa declaração é verdade para os casos em que $\mathbf{N}$ é o conjunto dos inteiros positivos. Em outras palavras, não existe um inteiro positivo n para o qual $n^2 < n$.

Funções Proposicionais com mais de uma Variável

Uma função proposicional (de n variáveis) definida em um conjunto produto $A = A_1 \times \ldots \times A_n$ é uma expressão

$$p(x_1, x_2, \ldots, x_n)$$

que tem a propriedade que $p(a_1, a_2, \ldots, a_n)$ é verdadeira ou falsa para uma n-upla $(a_1, \ldots a_n)$ em A. Por exemplo,

$$x + 2y + 3z < 18$$

é uma função proposicional em $\mathbf{N}^3 = \mathbf{N} \times \mathbf{N} \times \mathbf{N}$. Uma função proposicional não tem valor lógico. Entretanto, temos o seguinte:

Princípio básico: Uma função proposicional precedida por um quantificador para cada variável, por exemplo,

$$\forall x\, \exists y,\ p(x, y) \qquad \text{ou} \qquad \exists x\ \forall y\, \exists z,\ p(x, y, z)$$

é uma declaração e tem valor lógico.

Exemplo 4.14 Seja $B = \{1, 2, 3, \ldots, 9\}$, e seja $p(x, y)$ a fórmula "$x + y = 10$". Então, $p(x, y)$ é uma função proposicional em $A = B^2 = B \times B$.

(*a*) A sentença seguinte é uma declaração, pois existe um quantificador para cada variável:

$$\forall x\, \exists y,\ p(x, y),\ \text{isto é, "Para todo } x\text{, existe um } y \text{ tal que } x + y = 10\text{".}$$

Essa declaração é verdadeira. Por exemplo, se $x = 1$, seja $y = 9$; se $x = 2$, seja $y = 8$, e assim por diante.

(*b*) A sentença seguinte também é uma declaração:

$$\exists\, y \forall x,\ p(x, y),\ \text{isto é, "Existe um } y \text{ tal que, para todo } x\text{, temos } x + y = 10\text{".}$$

Não existe um tal y; portanto, a declaração é falsa.

Note que a única diferença entre (*a*) e (*b*) é a ordem dos quantificadores. Logo, uma ordenação diferente nos quantificadores gera uma declaração distinta. Observamos que, ao traduzir esses quantificadores para a linguagem usual, a expressão "tal que" freqüentemente segue "existe".

Negação de Declarações com Quantificadores com mais de uma Variável

Declarações com quantificadores com mais de uma variável podem ser negadas pela aplicação sucessiva dos Teoremas 4.5 e 4.6. Portanto, cada $\forall$ é transformado em $\exists$, e cada $\exists$ é mudado para $\forall$ quando o símbolo de negação $\neg$ é colocado na declaração da esquerda para a direita. Por exemplo,

$$\begin{aligned}\neg[\forall x \exists y \exists z, p(x, y, z)] &\equiv \exists x \neg[\exists y \exists z, p(x, y, z)] \equiv \exists x \forall y[\neg \exists z, p(x, y, z) \\ &\equiv \exists x \, \forall y \, \forall z, \ \neg p(x, y, z)\end{aligned}$$

Naturalmente, não indicamos todos os passos quando negamos uma declaração.

Exemplo 4.15

(*a*) Considere a declaração quantificada:

"Todo estudante faz pelo menos um curso em que o palestrante é um professor assistente."

Sua negação é a declaração:

"Existe um estudante tal que em todo curso o palestrante não é um professor assistente."

(*b*) A definição formal de que L é o limite de uma seqüência $a_1, a_2, \ldots$ é a seguinte:

$$\forall \in > 0, \exists n_0 \in \mathbf{N}, \quad \forall n > n_0, \quad |a_n - L| < \in$$

Portanto, L não é o limite de uma seqüência $a_1, a_2, \ldots$ quando:

$$\exists \in > 0, \quad \forall n_0 \in \mathbf{N}, \quad \exists n > n_0, \quad |a_n - L| \geq \in$$

Problemas Resolvidos

4.1 Seja p a sentença "Faz frio" e q a sentença "Chove". Dê uma sentença verbal simples que descreve cada uma das proposições a seguir: (*a*) $\neg p$; (*b*) $p \wedge q$; (*c*) $p \vee q$; (*d*) $q \vee \neg p$.

Em cada caso, traduza $\wedge$, $\vee$ e $\neg$ por "e", "ou" e "é falso que" ou "não", respectivamente, e então simplifique a sentença.

(*a*) Não faz frio.

(*b*) Faz frio e chove.

(*c*) Faz frio ou chove.

(*d*) Chove ou não faz frio.

4.2 Seja p a sentença "Érico lê *Newsweek*", q a sentença "Érico lê *The New Yorker*" e r "Érico lê *Time*". Escreva cada uma das seguintes declarações na forma simbólica:

(*a*) Érico lê *Newsweek* ou *The New Yorker*, mas não *Time*.

(*b*) Érico lê *Newsweek* e *The New Yorker*, ou ele não lê *Newsweek* e *Time*.

(*c*) Não é verdade que Érico lê *Newsweek*, mas não *Time*.

(*d*) Não é verdade que Érico lê *Time* ou *The New Yorker*, mas não *Newsweek*.

Use $\vee$ para "ou", $\wedge$ para "e" e $\neg$ para "não" (negação).

(*a*) $(p \vee q) \wedge \neg r$; (*b*) $(p \wedge q) \vee \neg (p \wedge r)$; (*c*) $\neg (p \wedge \neg r)$; (*d*) $\neg [(r \vee q) \wedge \neg p]$.

Tabelas-Verdade e Valores Lógicos

4.3 Determine o valor lógico de cada uma das declarações seguintes:

(*a*) $4 + 2 = 5$ e $6 + 3 = 9$.

(*b*) $3 + 2 = 5$ e $6 + 1 = 7$.

(*c*) $4 + 5 = 9$ e $1 + 2 = 4$.

(*d*) $3 + 2 = 5$ e $4 + 7 = 11$.

A declaração "p e q" é verdade apenas quando ambas as subdeclarações são verdade. Portanto: (*a*) falso; (*b*) verdadeiro; (*c*) falso; (*d*) verdadeiro.

4.4 Ache a tabela-verdade de $\neg p \wedge q$.

Veja a Figura 4-12, que apresenta ambos os métodos para construir uma tabela-verdade.

p	q	$\neg p$	$\neg p \wedge q$
V	V	F	F
V	F	F	F
F	V	V	V
F	F	V	F

(*a*) Método 1

p	q	$\neg$	p	$\wedge$	q
V	V	F	V	F	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	F	F	F
Passos		2	1	3	1

(*b*) Método 2

Fig. 4-12

4.5 Verifique que a proposição $p \vee \neg (p \wedge q)$ é uma tautologia.

Construa a tabela-verdade de $p \vee \neg (p \wedge q)$ como mostrado na Figura 4-13. Como o valor lógico de $p \vee \neg (p \wedge q)$ é V para todos os valores de p e q, a proposição é uma tautologia.

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

Fig. 4-13

4.6 Mostre que as proposições $\neg (p \wedge q)$ e $\neg p \vee \neg q$ são logicamente equivalentes.

Construa as tabelas-verdade para $\neg (p \wedge q)$ e $\neg p \vee \neg q$ como na Figura 4-14. Como as tabelas-verdade são iguais (ambas as proposições são falsas no primeiro caso e verdadeiras nos outros três), as proposições $\neg (p \wedge q)$ e $\neg p \vee \neg q$ são logicamente equivalentes, e podemos escrever

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

p	q	$p \wedge q$	$\neg (p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

(*a*) $\neg (p \wedge q)$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	F	F	F
V	F	F	V	V
F	V	V	F	V
F	F	V	V	V

(*b*) $\neg p \vee \neg q$

Fig. 4-14

4.7 Use as leis da Tabela 4-1 para mostrar que $\neg (p \vee q) \vee (\neg p \wedge q) \equiv \neg p$.

	Declaração	Razão
(1)	$\neg (p \vee q) \vee (\neg p \wedge q) \equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q)$	Lei de DeMorgan
(2)	$\equiv \neg p \wedge (\neg q \vee q)$	Lei de distributividade
(3)	$\equiv \neg p \wedge V$	Lei dos complementares
(4)	$\equiv \neg p$	Lei de identidade

Declarações Condicionais

4.8 Rescreva as declarações seguintes sem usar o condicional.

(*a*) Se está frio, ele usa chapéu.

(*b*) Se a produtividade cresce, o salário aumenta.

Lembre que "se p então q" é equivalente a "não p ou q" isto é, $p \rightarrow q \equiv \neg p \vee q$. Portanto,

(*a*) Não está frio ou ele usa um chapéu.

(*b*) A produtividade não cresce ou o salário aumenta.

4.9 Determine a contrapositiva de cada declaração.

(*a*) Se João é um poeta, então ele é pobre.

(*b*) Apenas se Marcos estudar, ele passará no teste.

(*a*) A contrapositiva de $p \rightarrow q$ é $\neg q \rightarrow \neg p$. Portanto, a contrapositiva da declaração dada é

Se João não é pobre, então ele não é poeta.

(*b*) A declaração dada é equivalente a "Se Marcos passar no teste, então ele estudou". Portanto, a contrapositiva é

Se Marcos não estudar, então não passará no teste.

4.10 Considere a proposição condicional $p \rightarrow q$. As proposições simples $q \rightarrow p$, $\neg p \rightarrow \neg q$ e $\neg q \rightarrow \neg p$ são chamadas, respectivamente, *conversa*, *inversa* e *contrapositiva* da proposição condicional $p \rightarrow q$. Quais destas, se existir alguma, é equivalente a $p \rightarrow q$?

Construa as tabelas-verdade como na Figura 4-15. Apenas a contrapositiva $\neg q \rightarrow \neg p$ é logicamente equivalente à proposição condicional original $p \rightarrow q$.

				Condicional	Conversa	Inversa	Contrapositiva
p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$q \rightarrow p$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
V	V	F	F	V	V	V	V
V	F	F	V	F	V	V	F
F	V	V	F	V	F	F	V
F	F	V	V	V	V	V	V

Fig. 4-15

4.11 Escreva a negação de cada declaração da forma mais simples possível.

(*a*) Se ela trabalhar, ganhará dinheiro.

(*b*) Ele nada se e somente se a água está morna.

(*c*) Se nevar, então eles não dirigem.

(*a*) Note que $\neg (p \rightarrow q) \equiv p \wedge \neg q$; portanto, a negação da declaração é:

Ela trabalhará ou não ganhará dinheiro.

(*b*) Note que $\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$; portanto, a negação da declaração é uma das seguintes:

Ele nada se e somente se a água não está morna.

Ele não nada se e somente se a água não está morna.

(*c*) Note que $\neg (p \rightarrow \neg q) \equiv p \wedge \neg \neg q \equiv p \wedge q$. Portanto, a negação da declaração é:

Neva e eles dirigem.

Argumentos

4.12 Mostre que o argumento seguinte é uma falácia: $p \rightarrow q,\ \neg p \vdash \neg q$.

Construa a tabela-verdade para $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ como na Figura 4-16. Como a proposição $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ não é uma tautologia, o argumento é uma falácia. Equivalentemente, o argumento é uma falácia uma vez que, na terceira linha da tabela-verdade, $p \rightarrow q$ e $\neg p$ é verdade, mas $\neg q$ é falso.

p	q	$p \rightarrow q$	$\neg p$	$(p \rightarrow q) \wedge \neg p$	$\neg q$	$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$
V	V	V	F	F	F	V
V	F	F	F	F	V	V
F	V	V	V	V	F	F
F	F	V	V	V	V	V

Fig. 4-16

4.13 Determine a validade do seguinte argumento: $p \rightarrow q,\ \neg q \vdash \neg p$.

Construa a tabela-verdade para $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ como na Figura 4-17. Como a proposição $[(p \rightarrow q) \wedge \neg q] \rightarrow \neg p$ é uma tautologia, o argumento é válido.

p	q	$[(p$	$\rightarrow$	$q)$	$\wedge$	$\neg$	$q]$	$\rightarrow$	$\neg$	p
V	V	V	V	V	F	F	V	V	F	V
V	F	V	F	F	F	V	F	V	F	V
F	V	F	V	V	F	F	V	V	V	F
F	F	F	V	F	V	V	F	V	V	F
Passos		1	2	1	3	2	1	4	2	1

Fig. 4-17

4.14 Prove que o seguinte argumento é válido: $p \rightarrow \neg q,\ r \rightarrow q,\ r \vdash \neg p$.

Construa as tabelas-verdade das premissas e da conclusão como na Figura 4-18. Agora, $p \rightarrow \neg q$, $r \rightarrow q$ e r são simultaneamente verdade apenas na quinta linha da tabela, onde $\neg p$ também é verdade. Portanto, o argumento é válido.

	p	q	r	$p \rightarrow \neg q$	$r \rightarrow q$	$\neg q$
1	V	V	V	F	V	F
2	V	V	F	F	V	F
3	V	F	V	V	F	F
4	V	F	F	V	V	F
5	F	V	V	V	V	V
6	F	V	F	V	V	V
7	F	F	V	V	F	V
8	F	F	F	V	V	V

Fig. 4-18

4.15 Teste a validade do argumento seguinte:

Se dois lados de um triângulo são iguais, então os ângulos opostos são iguais.
Dois lados de um triângulo não são iguais.

Os ângulos opostos não são iguais.

Primeiramente traduza o argumento na forma simbólica $p \rightarrow q,\ \neg p \vdash \neg q$, onde p é "Dois lados de um triângulo são iguais", e q é "Os ângulos opostos são iguais". Pelo Problema 4.12, o argumento é uma falácia.

Observação: Embora a conclusão siga da segunda premissa e dos axiomas da geometria euclidiana, o argumento acima não se constitui em uma prova, já que é uma falácia.

4.16 Determine a validade do seguinte argumento:

Se 7 é menor do que 4, então 7 não é um número primo.
7 não é menor do que 4.

---

7 é um número primo.

Primeiramente traduza o argumento na forma simbólica. Seja p a proposição "7 é menor do que 4", e seja q a proposição "7 é um número primo". Então, o argumento é da forma

$$p \to \neg q,\ \neg p \vdash q$$

Agora construímos a tabela-verdade como mostrado na Figura 4-19. Fica provado que o argumento acima é uma falácia, já que, na quarta linha da tabela-verdade, as premissas $p \to \neg q$ e $\neg p$ são verdade, mas a conclusão q é falsa.

Observação: O fato de que a conclusão do argumento é uma declaração verdadeira é irrelevante para o fato de que o argumento é uma falácia.

p	q	$\neg q$	$p \to \neg q$	$\neg p$
V	V	F	F	F
V	F	V	V	F
F	V	F	V	V
F	F	V	V	V

Fig. 4-19

Quantificadores e Funções Proposicionais

4.17 Seja $A = \{1, 2, 3, 4, 5\}$. Determine o valor lógico de cada uma das declarações seguintes:

(*a*) $(\exists x \in A)(x + 3 = 10)$ (*b*) $(\forall x \in A)(x + 3 < 10)$

(*c*) $(\exists x \in A)(x + 3 < 5)$ (*d*) $(\forall x \in A)(x + 3 \leq 7)$

(*a*) Falsa. Nenhum número em A é uma solução de $x + 3 = 10$.

(*b*) Verdadeira. Todo número em A satisfaz $x + 3 < 10$.

(*c*) Verdadeira. Se $x_0 = 1$, então $x_0 + 3 < 5$, i. e., 1 é uma solução.

(*d*) Falsa. Se $x_0 = 5$, então $x_0 + 3$ não é menor ou igual a 7. Em outras palavras, 5 não é uma solução da equação dada.

4.18 Determine o valor lógico de cada uma das declarações seguintes, onde $\mathbf{U} = \{1, 2, 3\}$ é o conjunto universo: (*a*) $\exists x\ \forall y, x^2 < y + 1$; (*b*) $\forall x\ \exists y, x^2 + y^2 < 12$; (*c*) $\forall x\ \forall y, x^2 + y^2 < 12$.

(*a*) Verdadeira. Se $x = 1$, então 1, 2 e 3 são soluções de $1 < y + 1$.

(*b*) Verdadeira. Para cada x_0, seja $y = 1$; então $x_0^2 + 1 < 12$ é uma declaração verdadeira.

(*c*) Falsa. Se $x_0 = 2$ e $y_0 = 3$, então $x_0^2 + y_0^2 < 12$ não é uma declaração verdadeira.

4.19 Negue cada uma das declarações seguintes:

(*a*) $\exists x\ \forall y,\ p(x, y)$; (*b*) $\exists x \forall y,\ p(x, y)$; (*c*) $\exists y\ \exists x\ \forall z,\ p(x, y, z)$.

Use $\neg \forall x\, p(x) \equiv \exists x\, \neg p(x)$ e $\neg \exists x\, p(x) \equiv \forall x\, \neg p(x)$:

(*a*) $\neg (\exists x\ \forall y,\ p(x, y)) \equiv \forall x\ \exists y\ \neg p(x, y)$.

(*b*) $\neg (\forall x\ \forall y,\ p(x, y)) \equiv \exists x\ \exists y\ \neg p(x, y)$.

(*c*) $\neg (\exists y\ \exists x\ \forall z,\ p(x, y, z)) \equiv \forall y\ \forall x\ \exists z\ \neg p(x, y, z)$.

4.20 Seja $p(x)$ a sentença "$x + 2 = 5$". Diga se $p(x)$ é uma função proposicional em cada um dos seguintes conjuntos: (*a*) **N**, o conjunto dos inteiros positivos; (*b*) $M = \{-1, -2, -3 \ldots\}$; (*c*) **C**, o conjunto dos números complexos.

(*a*) Sim.

(*b*) Embora $p(x)$ seja falsa para todo elemento em M, $p(x)$ é uma função proposicional em M.

(*c*) Não. Note que $2i + 2 > 5$ não tem qualquer significado. Em outras palavras, desigualdades não são definidas para números complexos.

4.21 Negue cada uma das declarações seguintes: (*a*) Todos os estudantes moram em dormitórios. (*b*) Todos os grandes matemáticos são do sexo masculino. (*c*) Alguns estudantes têm 25 anos de idade ou mais.

Use o Teorema 4.5 para negar os quantificadores.

(*a*) Pelo menos um estudante não mora em dormitório. (Alguns estudantes não moram em dormitórios.)

(*b*) Pelo menos um grande matemático é do sexo feminino. (Alguns grandes matemáticos são do sexo feminino.)

(*c*) Nenhum estudante tem 25 anos ou mais. (Todos os estudantes têm menos de 25 anos.)

Problemas Complementares

Proposições e Operações Lógicas

4.22 Seja p a sentença "Adriana fala francês" e, q a sentença "Adriana fala dinamarquês". Dê uma sentença verbal simples que descreva cada uma das seguintes:

$$(a)\ p \vee q; \quad (b)\ p \wedge q; \quad (c)\ p \wedge \neg q; \quad (d)\ \neg p \vee \neg q; \quad (e)\ \neg \neg p; \quad (f)\ \neg(\neg p \wedge \neg q).$$

4.23 Denote por p a declaração "Ele é rico" e por q a declaração "Ele é alegre". Escreva cada declaração na forma simbólica usando p e q. Note que "Ele é pobre" e "Ele é triste" são equivalentes a $\neg p$ e $\neg q$, respectivamente.

(*a*) Se ele é rico, então ele é triste.

(*b*) Ele não é nem rico nem alegre.

(*c*) É necessário ser pobre para ser alegre.

(*d*) Ser pobre é ser triste.

4.24 Ache as tabelas-verdade para: (*a*) $p \vee \neg q$; (*b*) $\neg p \wedge \neg q$.

4.25 Verifique que a proposição $(p \wedge q) \wedge \neg (p \vee q)$ é uma contradição.

Argumentos

4.26 Teste a validade de cada argumento:

(*a*) Se chover, Érico ficará doente.
Não choveu.

Érico não ficou doente.

(*b*) Se chover, Érico ficará doente.
Érico não ficou doente

Não choveu.

4.27 Teste a validade do seguinte argumento:

Se eu estudar, não serei reprovado em matemática.
Se eu não jogar basquete, então vou estudar.
Fui reprovado em matemática.

Portanto, devo ter jogado basquete.

4.28 Mostre que: (*a*) $p \wedge q$ implica logicamente $p \leftrightarrow q$, (*b*) $p \leftrightarrow \neg q$ não implica logicamente $p \rightarrow q$.

Quantificadores

4.29 Seja $A = \{1, 2, \ldots, 9, 10\}$. Considere cada uma das sentenças seguintes. Se for uma declaração, determine seu valor lógico. Se for uma função proposicional, determine seu conjunto verdade.

(*a*) $(\forall x \in A)(\exists y \in A)(x + y < 14)$.
(*b*) $(\forall y \in A)(x + y < 14)$.
(*c*) $(\forall x \in A)(\forall y \in A)(x + y < 14)$.
(*d*) $(\exists y \in A)(x + y < 14)$.

4.30 Negue cada uma das declarações seguintes:

(*a*) Se a professora está ausente, então alguns estudantes não terminam seu dever de casa.

(*b*) Todos os estudantes terminaram seu dever de casa e a professora está presente.

(*c*) Alguns dos estudantes não terminaram seu dever de casa ou a professora está ausente.

4.31 Negue cada uma das declarações no Problema 4.17.

4.32 Ache um contra-exemplo para cada declaração onde $\mathbf{U} = \{3, 5, 7, 9\}$ é o conjunto universo. (*a*) $\forall x, x + 3 \geq 7$; (*b*) $\forall x$, x é ímpar ; (*c*) $\forall x$, x é primo; ; (*d*) $\forall x, |x| = x$.

Respostas dos Problemas Complementares

4.22 Em cada caso, substitua $\wedge$, $\vee$ e $\neg$ por "e", "ou" e "é falso que" ou "não", respectivamente, e então simplifique a sentença em português.

(*a*) Adriana fala francês ou dinamarquês.

(*b*) Adriana fala francês e dinamarquês.

(*c*) Adriana fala francês, mas não dinamarquês.

(*d*) Adriana não fala francês ou não fala dinamarquês.

(*e*) Não é verdade que Adriana não fala inglês.

(*f*) Não é verdade que Adriana não fala nem francês nem dinamarquês.

4.23 (*a*) $p \rightarrow \neg q$; (*b*) $\neg p \wedge \neg q$; (*c*) $q \rightarrow \neg p$; (*d*) $\neg p \leftrightarrow \neg q$.

4.24 As tabelas-verdade aparecem na Figura 4-20.

p	q	$\neg q$	$p \vee \neg q$
V	V	F	V
V	F	V	V
F	V	F	F
F	F	V	V

(*a*)

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
V	V	F	F	F
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

(*b*)

Fig. 4-20

4.25 É uma contradição, já que sua tabela-verdade na Figura 4-21 é falsa para todos os valores de p e q.

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

Fig. 4-21

4.26 Primeiramente traduza os argumentos na forma simbólica, escolha p para "Se chover" e q para "Érico está doente", como a seguir:

$$(a)\ p \rightarrow q,\ \neg p \vdash \neg q, \qquad (b)\ p \rightarrow q,\ \neg q \vdash \neg p$$

Pelo Problema 4.12, o argumento (*a*) é uma falácia. Pelo Problema 4-13, o argumento (*b*) é válido.

4.27 Seja p a declaração "Eu estudo", q a declaração "Eu sou reprovado em matemática" e r "Eu jogo basquete", o argumento dado tem a forma:

$$p \to \neg q,\ \neg r \to p, q \vdash r$$

Construa as tabelas-verdade como na Figura 4-22, onde as premissas $p \to \neg q$, $\neg r \to p$ e q são simultaneamente verdadeiras apenas na quinta linha da tabela e, neste caso, a conclusão r também é verdadeira. Portanto, o argumento é válido.

p	q	r	$\neg q$	$p \to \neg q$	$\neg r$	$\neg r \to p$
V	V	V	F	F	F	V
V	V	F	F	F	V	V
V	F	V	V	V	F	V
V	F	F	V	V	V	V
F	V	V	F	V	F	V
F	V	F	F	V	V	F
F	F	V	V	V	F	V
F	F	F	V	V	V	F

Fig. 4-22

4.28 (*a*) Construa as tabelas-verdade de $p \wedge q$ e $p \leftrightarrow q$ como na Figura 4-23(*a*). Note que $p \wedge q$ é verdadeira apenas na primeira linha da tabela, onde $p \leftrightarrow q$ também é verdade

(*b*) Construa as tabelas-verdade de $p \leftrightarrow \neg q$ e $p \to q$ como na Figura 4-23(*b*). Note que $p \leftrightarrow \neg q$ é verdadeira na segunda linha da tabela, onde $p \to q$ é falsa.

p	q	$p \wedge q$	$p \leftrightarrow q$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	F	V

(*a*)

p	q	$\neg q$	$p \leftrightarrow \neg q$	$p \to q$
V	V	F	F	V
V	F	V	V	F
F	V	F	V	V
F	F	V	F	V

(*b*)

Fig. 4-23

4.29 (*a*) A sentença aberta em duas variáveis é precedida por dois quantificadores; portanto, é uma declaração. Ademais, a declaração é verdadeira.

(*b*) A sentença aberta é precedida por um quantificador; portanto, é uma função proposicional na outra variável. Note que, para cada $y \in A$, $x_0 + y < 14$ se e somente se $x_0 = 1, 2$ ou 3. Logo, o conjunto verdade é $\{1, 2, 3\}$.

(*c*) É uma declaração e é falsa; se $x_0 = 8$ e $y_0 = 9$, então $x_0 + y_0 < 14$ não é verdade.

(*d*) É uma sentença aberta em x. O conjunto verdade é o próprio A.

4.30 (*a*) A professora está ausente e todos os estudantes terminaram o seu dever de casa.

(*b*) Alguns estudantes não terminaram o seu dever de casa ou a professora está ausente.

(*c*) Todos os estudantes terminaram o seu dever de casa e a professora está presente.

4.31 (*a*) $(\forall x \in A)(x + 3 \neq 10)$.

(*b*) $(\exists x \in A)(x + 3 \geq 10)$.

(*c*) $(\forall x \in A)(x + 3 \geq 5)$.

(*d*) $(\exists x \in A)(x + 3 > 7)$.

4.32 (*a*) Neste caso, 5, 7 e 9 são contra-exemplos.

(*b*) A declaração é verdade; portanto não existe contra-exemplo.

(*c*) Aqui, 9 é o único contra-exemplo.

(*d*) A declaração é verdadeira; portanto, não existe contra-exemplo.

Capítulo 5

Vetores e Matrizes

5.1 INTRODUÇÃO

Dados são freqüentemente organizados em *arrays*[†], isto é, conjuntos cujos elementos são indexados por um ou mais índices. Normalmente, um *array* unidimensional é chamado de vetor, e um *array* bidimensional é chamado de matriz. (A dimensão, neste caso, denota o número de índices.) Apresentamos aqui a motivação para estas estruturas e sua notação.

Suponha que os pesos (em libras) de oito estudantes sejam listados como a seguir:

$$134, \quad 156, \quad 127, \quad 145, \quad 203, \quad 186, \quad 145, \quad 138$$

Pode-se denotar todos os valores na lista inserindo apenas um símbolo, w, com índices diferentes.

$$w_1, \quad w_2, \quad w_3, \quad w_4, \quad w_5, \quad w_6, \quad w_7, \quad w_8$$

Observe que cada índice denota uma posição do valor na lista. Por exemplo,

$$w_1 = 134, \text{ o primeiro número;} \qquad w_2 = 156, \text{ o segundo número; } \ldots$$

Essa lista de valores é dita um *vetor* ou *array linear*.

Usando a notação de índices, pode-se escrever a soma S e a média dos pesos, A, como a seguir:

$$S = \sum_{k=1}^{8} w_k = w_1 + w_2 + \ldots + w_8 \qquad \text{e} \qquad A = \frac{S}{8} = \frac{1}{8}\left[\sum_{k=1}^{8} w_k\right]$$

A notação utilizando índices é indispensável no desenvolvimento de expressões concisas para manipulações aritméticas de listas de valores.

De maneira similar, uma cadeia de 28 lojas, cada loja com quatro departamentos, poderia listar suas vendas semanais (com valores aproximados, em dólares) como na Tabela 5-1. Precisamos de apenas um símbolo, digamos s, com dois índices para denotar todos os valores na tabela.

$$s_{1,1}, \quad s_{1,2}, \quad s_{1,3}, \quad s_{1,4}, \quad s_{2,1}, \quad s_{2,2}, \quad \ldots, \quad s_{28,4}$$

[†] N. de T. Em português, às vezes se usa a tradução "vetor", mas a palavra *array* é mais freqüente nos textos de ciência da computação e áreas afins.

onde $s_{i,j}$ denota as vendas na loja i, departamento j. (Escrevemos s_{ij} em vez de $s_{i,j}$ quando não houver possibilidade de mal-entendidos). Portanto,

$$s_{11} = \$2872, \quad s_{12} = \$805, \quad s_{13} = \$3211, \quad \ldots$$

Um *array* retangular de números como este é denominado *matriz* ou *array bidimensional*.

Este capítulo investiga vetores e matrizes e certas operações algébricas envolvendo-os. Neste contexto, os números em si são ditos *escalares*.

Tabela 5-1

Loja \ Dep.	1	2	3	4
1	2872	805	3211	1560
2	2196	1223	2525	1744
3	3257	1017	3686	1951
. . .	. . .	. . .	. . .	. . .
28	2618	931	2333	982

5.2 VETORES

Vamos nos referenciar a uma lista de números, $a_1, a_2, \ldots, a_n$, como um *vetor* u. Um tal vetor é denotado por

$$u = (a_1, a_2, \ldots, a_n)$$

Os números a_i são ditos *componentes* ou *elementos* de u. Se todos os $a_i = 0$, então u é dito o *vetor zero*. Dois vetores u e v são *iguais* (escreve-se $u = v$) se têm o mesmo número de componentes e os componentes correspondentes são iguais.

Exemplo 5.1

(*a*) São vetores:

$$(3, -4) \qquad (6, 8) \qquad (0, 0, 0) \qquad (2, 3, 4)$$

Os dois primeiros vetores têm dois componentes, enquanto os dois últimos têm três. O terceiro vetor é o vetor zero com três componentes.

(*b*) Embora os vetores (1, 2, 3) e (2, 3, 1) contenham os mesmos números, eles não são iguais, pois os componentes correspondentes não são iguais.

Operações com Vetores

Considere dois vetores arbitrários u e v com o mesmo número de componentes,

$$u = (a_1, a_2, \ldots, a_n) \qquad \text{e} \qquad v = (b_1, b_2, \ldots, b_n)$$

A *soma* de u e v (escreve-se $u + v$) é o vetor obtido pela adição dos componentes correspondentes de u e v, isto é,

$$u + v = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

O *produto por escalar* ou, simplesmente, *produto*, de um escalar k e um vetor u (escreve-se ku) é o vetor obtido pela multiplicação de cada componente de u por k; isto é,

$$ku = (ka_1, ka_2, \ldots, ka_n)$$

Também definimos

$$-u \equiv -1(u) \qquad \text{e} \qquad u - v = u + (-v)$$

e escolhemos 0 para denotar o vetor zero. O vetor $-u$ é dito o *negativo* do vetor u.

O *produto interno* dos vetores u e v descritos acima é denotado e definido por

$$u \cdot v = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

A *norma*, ou *comprimento*, do vetor u é denotada e definida por

$$\|u\| = \sqrt{u \cdot u} = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$$

Notamos que $\|u\| = 0$ se e somente se $u = 0$; caso contrário, $\|u\| > 0$.

Exemplo 5.2 Seja $u = (2, 3, -4)$ e $v = (1, -5, 8)$. Então,

$$\begin{aligned} u + v &= (2 + 1, 3 - 5, -4 + 8) = (3, -2, 4) \\ 5u &= (5 \cdot 2,\ 5 \cdot 3,\ 5 \cdot (-4)) = (10, 15, -20) \\ -v &= -1 \cdot (1, -5, 8) = (-1, 5, -8) \\ 2u - 3v &= (4, 6, -8) + (-3, 15, -24) = (1, 21, -32) \\ u \cdot v &= 2 \cdot 1 + 3 \cdot (-5) + (-4) \cdot 8 = 2 - 15 - 32 = -45 \\ \|u\| &= \sqrt{2^2 + 3^2 + (-4)^2} = \sqrt{4 + 9 + 16} = \sqrt{29} \end{aligned}$$

Vetores, considerados conjuntamente com as operações de adição de vetores e produto por escalar, têm várias propriedades, por exemplo,

$$k(u + v) = ku + kv$$

onde k é um escalar, e u e v são vetores. Muitas dessas propriedades aparecem no Teorema 5.1 (veja a Seção 5.4), que também vale para vetores, uma vez que estes podem ser encarados como um caso particular de matrizes.

Vetores Coluna

Às vezes uma lista de números é escrita no sentido vertical em vez de horizontal, sendo chamada *vetor coluna*. Neste contexto, os vetores escritos no sentido horizontal acima são chamados *vetores linha*. As operações acima para vetores linha são definidas de maneira análoga para vetores coluna.

Exemplo 5.3

(*a*) São vetores coluna:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 \\ -3 \end{bmatrix}, \qquad \begin{bmatrix} 1 \\ 2 \\ -6 \end{bmatrix}, \qquad \begin{bmatrix} 1{,}4 \\ \frac{3}{4} \\ -19 \end{bmatrix}$$

Os primeiros dois vetores têm dois componentes, enquanto os últimos dois têm três.

(*b*) Sejam

$$u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} \qquad \text{e} \qquad v = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$$

Então,

$$2u - 3v = \begin{bmatrix} 10 \\ 6 \\ -8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \\ -2 \end{bmatrix}$$

$$u \cdot v = 15 - 3 + 8 = 20 \qquad \text{e} \qquad \|u\| = \sqrt{25 + 9 + 16} = \sqrt{50} = 5\sqrt{2}$$

5.3 MATRIZES

Uma *matriz A* é um *array* retangular de números, normalmente representado na forma

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

As m listas horizontais de números são chamadas *linhas* de A, e as n listas verticais de números, suas *colunas*. Portanto, o elemento a_{ij}, chamado *elemento ij*, aparece na linha i e na coluna j. Freqüentemente denotamos uma matriz simplesmente escrevendo $A = [a_{ij}]$.

Uma matriz com m linhas e n colunas é dita uma matriz m por n (escreve-se $m \times n$). O par de números m e n é dito a *dimensão*[†] da matriz. Duas matrizes A e B são iguais se têm a mesma dimensão e se os seus elementos correspondentes são iguais. Portanto, a igualdade de duas matrizes $m \times n$ é equivalente a um sistema de mn igualdades, uma para cada par de elementos correspondentes.

Uma matriz com apenas uma linha é dita uma *matriz linha* ou *vetor linha*, e uma matriz com apenas uma coluna é dita uma *matriz coluna* ou *vetor coluna*. Uma matriz cujos elementos são todos zero é chamada *matriz zero* e será normalmente denotada por 0.

Exemplo 5.4

(*a*) O *array* retangular $A = \begin{bmatrix} 1 & -4 & 5 \\ 0 & 3 & -2 \end{bmatrix}$ é uma matriz 2×3. Suas linhas são $[1, -4, 5]$ e $[0, 3, -2]$ e suas colunas são $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} -4 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 5 \\ -2 \end{bmatrix}$.

(*b*) A matriz zero 2×4 é a matriz $0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(*c*) Suponha que

$$\begin{bmatrix} x+y & 2z+t \\ x-y & z-t \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 5 \end{bmatrix}$$

Então os quatro elementos correspondentes precisam ser iguais. Isto é,

$$x + y = 3, \qquad x - y = 1, \qquad 2z + t = 7, \qquad z - t = 5$$

A solução do sistema de equações é

$$x = 2, \qquad y = 1, \qquad z = 4, \qquad t = -1$$

5.4 ADIÇÃO DE MATRIZES E MULTIPLICAÇÃO POR ESCALAR

Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ duas matrizes de mesma dimensão, isto é, matrizes $m \times n$. A soma de A e B (escreve-se $A + B$) é a matriz obtida pela adição dos elementos correspondentes de A e B. Isto é,

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

[†] N. de T. No original, *size*.

O *produto* de uma matriz A por um escalar k (escreve-se $k \cdot A$, ou simplesmente kA) é a matriz obtida multiplicando-se cada elemento de A por k. Isto é,

$$kA = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ ka_{21} & ka_{22} & \cdots & ka_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ ka_{m1} & ka_{m2} & \cdots & ka_{mn} \end{bmatrix}$$

Observe que $A + B$ e kA são também matrizes $m \times n$. Também definimos

$$-A = (-1)A \qquad \text{e} \qquad A - B = A + (-B)$$

A matriz $-A$ é dita o *negativo* da matriz A. A soma de matrizes de dimensão diferentes não é definida.

Exemplo 5.5 Sejam $A = \begin{bmatrix} 1 & -2 & 3 \\ 0 & 4 & 5 \end{bmatrix}$ e $B = \begin{bmatrix} 4 & 6 & 8 \\ 1 & -3 & -7 \end{bmatrix}$. Então,

$$A + B = \begin{bmatrix} 1+4 & -2+6 & 3+8 \\ 0+1 & 4+(-3) & 5+(-7) \end{bmatrix} = \begin{bmatrix} 5 & 4 & 11 \\ 1 & 1 & -2 \end{bmatrix}$$

$$3A = \begin{bmatrix} 3(1) & 3(-2) & 3(3) \\ 3(0) & 3(4) & 3(5) \end{bmatrix} = \begin{bmatrix} 3 & -6 & 9 \\ 0 & 12 & 15 \end{bmatrix}$$

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 0 & 8 & 10 \end{bmatrix} + \begin{bmatrix} -12 & -18 & -24 \\ -3 & 9 & 21 \end{bmatrix} = \begin{bmatrix} -10 & -22 & -18 \\ -3 & 17 & 31 \end{bmatrix}$$

Matrizes consideradas conjuntamente com as operações de adição e multiplicação por escalar têm as propriedades a seguir.

Teorema 5-1: sejam A, B e C matrizes de mesma dimensão, e sejam k e k' escalares. Então:

(i) $(A + B) + C = A + (B + C)$
(ii) $A + 0 = 0 + A$
(iii) $A + (-A) = (-A) + 0 = A$
(iv) $A + B = B + A$
(v) $k(A + B) = kA + kB$.
(vi) $(k + k')A = kA + k'A$.
(vii) $(kk')A = k(k'A)$.
(viii) $1A = A$.

Note que o primeiro 0 em (ii) e (iii) se refere à matriz zero. Também por (i) e (iv), uma soma qualquer de matrizes

$$A_1 + A_2 + \cdots + A_n$$

não requer parênteses, e a soma não depende da ordem das matrizes. Ademais, usando (vi) e (viii), também temos

$$A + A = 2A, \qquad A + A + A = 3A, \qquad \ldots$$

Finalmente, já que um vetor com n componentes pode ser identificado com uma matriz $1 \times n$ ou $n \times 1$, o Teorema 5.1 também vale para vetores munidos das operações de adição e multiplicação por escalar.

A demonstração do Teorema 5.1 se reduz a mostrar que o elemento ij de cada matriz é igual em ambos os lados da equação. (Veja o Problema 5.10.)

5.5 MULTIPLICAÇÃO DE MATRIZES

O produto das matrizes A e B (escreve-se AB) é um pouco complicado. Por esta razão, começamos com um caso especial. (A Seção 3.5 apresenta uma discussão sobre o símbolo de somatório Σ, a letra grega sigma maiúscula.)

O produto AB de uma matriz linha $A = [a_i]$ e uma matriz coluna $B = [b_i]$ com o mesmo número de elementos é definido como a seguir:

$$AB = [a_1, a_2, \ldots, a_n]\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1b_1 + a_2b_2 + \cdots + a_nb_n = \sum_{k=1}^{n} a_kb_k$$

Isto é, AB é obtido multiplicando os elementos correspondentes em A e B e então adicionando todos os produtos. Enfatizamos que AB é um escalar (ou uma matriz 1×1). O produto AB não é definido quando A e B têm números diferentes de elementos.

Exemplo 5.6

(*a*) $[7, -4, 5]\begin{bmatrix} 3 \\ 2 \\ -1 \end{bmatrix} = 7(3) + (-4)(2) + 5(3) = 21 - 8 - 5 = 8$

(*b*) $[6, -1, 8, 3]\begin{bmatrix} 4 \\ -9 \\ -2 \\ 5 \end{bmatrix} = 24 + 9 - 16 + 15 = 32$

Agora estamos prontos para definir a multiplicação de matrizes em geral.

Definição: Suponha que $A = [a_{ik}]$ e $B = [b_{kj}]$ são matrizes, e que o número de colunas de A é igual ao número de linhas de B; isto é, A é uma matriz $m \times p$, e B é uma matriz $p \times n$. O produto AB é a matriz $m \times n$ cujo elemento ij é obtido pela multiplicação da i-ésima linha de A pela j-ésima coluna de B. Isto é,

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \cdot & \cdots & \cdot \\ a_{i1} & \cdots & a_{ip} \\ \cdot & \cdots & \cdot \\ a_{m1} & \cdots & a_{mp} \end{bmatrix}\begin{bmatrix} b_{11} & \cdots & b_{1j} & \cdots & b_{1n} \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ b_{p1} & \cdots & b_{pj} & \cdots & b_{pn} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \cdot & \cdots & \cdot \\ \cdot & c_{ij} & \cdot \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

onde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^{p} a_{ik}b_{kj}$$

Enfatizamos que o produto AB não é definido se A é uma matriz $m \times p$ e B é uma matriz $q \times n$ onde $p \neq q$.

Exemplo 5.7

(*a*) Ache AB onde $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 0 & -4 \\ 5 & -2 & 6 \end{bmatrix}$.

Como A é 2×2 e B é 2×3, o produto AB é definido, e AB é uma matriz 2×3. Para obter a primeira linha da matriz produto AB, multiplique a primeira linha $(1, 3)$ de A por cada coluna de B,

$$\begin{bmatrix} 2 \\ 5 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ -2 \end{bmatrix}, \quad \begin{bmatrix} -4 \\ 6 \end{bmatrix}$$

respectivamente. Isto é,

$$AB = \begin{bmatrix} 2 + 15 & 0 - 6 & -4 + 18 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \end{bmatrix}$$

Para obter a segunda linha do produto AB, multiplique a primeira linha $(2, -1)$ de A por cada coluna de B, respectivamente. Portanto,

$$AB = \begin{bmatrix} 17 & -6 & 14 \\ 4 - 5 & 0 + 2 & -8 - 6 \end{bmatrix} = \begin{bmatrix} 17 & -6 & 14 \\ -1 & 2 & -14 \end{bmatrix}$$

(*b*) Suponha que $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 5 & 6 \\ 0 & -2 \end{bmatrix}$. Então,

$$AB = \begin{bmatrix} 5+0 & 6-4 \\ 15+0 & 18-8 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 15 & 10 \end{bmatrix} \quad \text{e} \quad BA = \begin{bmatrix} 5+18 & 10+24 \\ 0-6 & 0-8 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ -6 & -8 \end{bmatrix}$$

O Exemplo 5.6(*b*) acima mostra que a multiplicação de matrizes não é comutativa, i.e., os produtos das matrizes AB e BA não são necessariamente iguais.

A multiplicação de matrizes satisfaz, entretanto, às seguintes propriedades:

Teorema 5-2: sejam A, B e C matrizes. Então, sempre que o produto e a soma estiverem definidos:

(i) $(AB)C = A(BC)$ (lei associativa).
(ii) $A(B+C) = AB + AC$ (lei distributiva pela esquerda).
(iii) $(B+C)A = BA + CA$ (lei distributiva pela direita).
(iv) $k(AB) = (kA)B = A(kB)$, onde k é um escalar.

Notamos que $0A = 0$ e $B0 = 0$, onde 0 é a matriz zero.

Multiplicação de Matrizes e Sistemas de Equações Lineares

Qualquer sistema S de equações lineares é equivalente à equação matricial

$$AX = B$$

onde A é a matriz que contém os coeficientes, X é o vetor coluna de incógnitas e B é o vetor coluna de constantes. (Aqui, *equivalente* quer dizer que qualquer solução do sistema S é uma solução da equação matricial $AX = B$ e vice-versa.) Por exemplo, o sistema

$$\begin{aligned} x + 2y - 3z &= 4 \\ 5x - 6y + 8z &= 9 \end{aligned} \qquad \text{é equivalente a} \qquad \begin{bmatrix} 1 & 2 & -3 \\ 5 & -6 & 8 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 4 \\ 9 \end{bmatrix}$$

Observe que o sistema é completamente determinado pela matriz

$$M = [A, B] = \begin{bmatrix} 1 & 2 & -3 & 4 \\ 5 & -6 & 8 & 9 \end{bmatrix}$$

que é chamada *matriz aumentada* do sistema.

5.6 TRANSPOSTA

A *transposta* de uma matriz A (escreve-se A^T) é a matriz obtida pela colocação das linhas de A, em ordem, no lugar das colunas. Por exemplo,

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix} \quad \text{e} \quad [1, -3, -5]^T = \begin{bmatrix} 1 \\ -3 \\ -5 \end{bmatrix}$$

Note que, se A é uma matriz $m \times n$, então A^T é uma matriz $n \times m$. Em particular, a transposta de um vetor linha é um vetor coluna e vice-versa. Ademais, se $B = [b_{ij}]$ é a transposta de $A = [a_{ij}]$, então $b_{ij} = a_{ji}$ para todos i e j.

A operação de transposição de matrizes satisfaz às seguintes propriedades.

Teorema 5-3: sejam A e B matrizes e seja k um escalar. Então, sempre que o produto e a soma estiverem definidos:

(i) $(A+B)^T = A^T + B^T$.
(ii) $(kA)^T = kA^T$, onde k é um escalar.
(iii) $(AB)^T = B^T A^T$.
(iv) $(A^T)^T = A$.

Enfatizamos que, por (iii), a transposta de um produto é o produto das transpostas, mas na ordem inversa.

5.7 MATRIZES QUADRADAS

Uma matriz com o mesmo número de linhas e colunas é chamada *matriz quadrada*. Uma matriz quadrada com n colunas e n linhas é dita de *ordem* n e é chamada matriz *n-quadrada*.

A *diagonal principal*, ou simplesmente *diagonal*, de uma matriz n-quadrada $A = [a_{ij}]$ consiste nos elementos $a_{11}, a_{22}, \ldots, a_{nn}$.

A *matriz unitária* n-quadrada, denotada por I_n ou simplesmente I, é a matriz quadrada com 1 ao longo da diagonal e zero nos outros elementos. A matriz unitária I desempenha um papel importante na multiplicação de matrizes, assim como o número 1 o faz na multiplicação usual de números. Especificamente

$$AI = IA = A$$

para qualquer matriz quadrada.

Considere, por exemplo, as matrizes

$$\begin{bmatrix} 1 & -2 & 0 \\ 0 & -4 & -6 \\ 5 & 3 & 2 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Ambas são matrizes quadradas. A primeira matriz é de ordem 3, e sua diagonal consiste nos elementos 1, –4 e 2. A segunda matriz é de ordem 4; sua diagonal consiste apenas em 1, e existem apenas zeros nas outras posições. Portanto, a segunda matriz é a matriz unitária de ordem 4.

Álgebra de Matrizes Quadradas

Seja A uma matriz quadrada qualquer. Podemos multiplicar A por ela mesma. Na verdade, podemos formar todas as *potências* não negativas de A como a seguir:

$$A^2 = AA, \qquad A^3 = A^2A, \qquad \ldots, \qquad A^{n+1} = A^nA, \qquad \ldots, \qquad \text{e} \qquad A^0 = I \text{ (quando } A \neq 0)$$

Também são definidos polinômios sobre a matriz A. Especificamente, para qualquer polinômio

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

onde os a_i são escalares, definimos $f(a)$ como sendo a matriz

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_nA^n$$

Note que $f(a)$ é obtida de $f(x)$ pela substituição da variável x pela matriz A e do termo escalar a_0 pela matriz a_0I. No caso em que $f(a)$ é a matriz zero, a matriz A é dita um *zero* ou uma *raiz* do polinômio $f(x)$.

Exemplo 5.8 Suponha que $A = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}$. Então,

$$A^2 = \begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} \qquad \text{e} \qquad A^3 = A^2A = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} = \begin{bmatrix} -11 & 38 \\ 57 & -106 \end{bmatrix}$$

Suponha que $f(x) = 2x^2 - 3x + 5$. Então,

$$f(A) = 2\begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} - 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 16 & -18 \\ -27 & 61 \end{bmatrix}$$

Suponha que $g(x) = x^2 + 3x - 10$. Então,

$$g(A) = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix} + 3\begin{bmatrix} 1 & 2 \\ 3 & -4 \end{bmatrix} - 10\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Portanto, A é um zero do polinômio $g(x)$.

5.8 MATRIZES INVERSÍVEIS (NÃO SINGULARES) E INVERSAS

Uma matriz quadrada A é dita ser *inversível* (*ou não singular*) se existe uma matriz B com a propriedade que

$$AB = BA = I, \text{ a matriz identidade.}$$

Uma tal matriz B é única (Problema 5.24); é chamada *inversa* de A e denotada por A^{-1}. Observe que B é a inversa de A se e somente se A é a inversa de B. Por exemplo, suponha que

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix} \qquad \text{e} \qquad B = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

Então,

$$AB = \begin{bmatrix} 6-5 & -10+10 \\ 3-3 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{e} \qquad BA = \begin{bmatrix} 6-5 & 15-15 \\ -2+2 & -5+6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Portanto, A e B são inversas.

É sabido que $AB = I$ se e somente se $BA = I$; portanto, é necessário testar apenas um produto para determinar se duas matrizes dadas são inversas, como no próximo exemplo.

Exemplo 5.9

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix} \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix} = \begin{bmatrix} -11+0+12 & 2+0-2 & 2+0-2 \\ -22+4+18 & 4+0-3 & 4-1-3 \\ -44-4+48 & 8+0-8 & 8+1-8 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Portanto, as duas matrizes são inversíveis e são inversa uma da outra.

5.9 DETERMINANTES

Para cada matriz n-quadrada $A = [a_{ij}]$, associamos um número específico chamado *determinante* de A e denotado por det (a) ou $|A|$ ou

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

Enfatizamos que um *array* quadrado de números, delimitado por linhas retas, chamado *determinante de ordem n*, não é uma matriz, mas denota o valor que a função determinante associa ao *array* de números, i.e., a matriz quadrada delimitada.

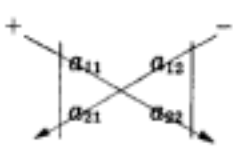
Os determinantes de ordem 1, 2 e 3 são definidos como a seguir:

$$|a_{11}| = a_{11}$$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

O diagrama seguinte pode ajudar o leitor a lembrar o determinante de ordem 2:



Isto é, o determinante é igual ao produto dos elementos ao longo da seta referenciada com sinal de adição menos o produto dos elementos ao longo da seta indicada com o sinal de subtração. Existe uma maneira análoga de lembrar o determinante de ordem 3. Por conveniência de notação, separamos as setas indicadas pelos sinais de soma e subtração.

Enfatizamos que não existem diagramas análogos para lembrar os determinantes de ordem superior.

Exemplo 5.10

$$(a)\ \begin{vmatrix} 5 & 4 \\ 2 & 3 \end{vmatrix} = 5(3) - 4(2) = 15 - 8 = 7, \qquad \begin{vmatrix} 2 & 1 \\ -4 & 6 \end{vmatrix} = 2(6) - 1(-4) = 12 + 4 = 16.$$

$$(b)\ \begin{vmatrix} 2 & 1 & 3 \\ 4 & 6 & -1 \\ 5 & 1 & 0 \end{vmatrix} = 2(6)(0) + 1(-1)(5) + 3(1)(4) - 3(6)(5) - 1(4)(0) - 2(1)(-1)$$
$$= 0 - 5 + 12 - 90 - 0 + 2 = -81.$$

Definição Geral de Determinantes

A definição geral de um determinante de ordem n é

$$\det(A) = \sum \operatorname{sgn}(\sigma) a_{1j_1} a_{2j_2} \cdots a_{nj_n}$$

onde a soma é efetuada sobre todas as permutações $\sigma = \{j_1, j_2, \ldots, j_n\}$ de $\{1, 2, \ldots, n\}$. Neste caso, sinal (σ) é igual a +1 ou −1 de acordo com a necessidade de um número par ou ímpar de trocas a fim de que σ esteja na ordem usual. Incluímos aqui a definição geral da função determinante para que o texto fique completo. O leitor deve se referenciar a textos de teoria de matrizes ou álgebra linear para técnicas de cálculo de determinantes de ordem maior do que 3. As permutações são estudadas no Capítulo 6.

Uma propriedade importante da função determinante é a de ser multiplicativa. Isto é,

Teorema 5-4: sejam A e B matrizes quaisquer n-quadradas. Então,

$$\det(AB) = \det(A) \cdot \det(B)$$

A demonstração do teorema acima está além do objetivo deste texto.

Determinantes e Inversas de Matrizes 2×2

Seja A uma matriz 2×2 arbitrária:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Queremos deduzir uma fórmula para A^{-1}, a inversa de A. Especificamente procuramos $2^2 = 4$ escalares, x_1, y_1, x_2, y_2, tais que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} ax_1 + by_1 & ax_2 + by_2 \\ cx_1 + dy_1 & cx_2 + dy_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Igualando os quatro elementos, respectivamente, aos elementos correspondentes na matriz identidade, obtêm-se quatro equações que podem ser divididas em dois sistemas 2×2 como a seguir:

$$ax_1 + by_1 = 1, \qquad ax_2 + by_2 = 0,$$
$$cx_1 + dy_1 = 0, \qquad cx_2 + dy_2 = 1$$

Observe que as matrizes aumentadas nos dois sistemas são as seguintes:

$$\begin{bmatrix} a & b & 1 \\ c & d & 0 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} a & b & 0 \\ c & d & 1 \end{bmatrix}$$

(Note que a matriz original A é a matriz dos coeficientes de ambos os sistemas.)

Suponha agora que $|A| = ad - bc \neq 0$. Então, podemos calcular a única solução dos dois sistemas de incógnitas, x_1, y_1, x_2, y_2, obtendo

$$x_1 = \frac{d}{ad-bc} = \frac{d}{|A|}, \qquad y_1 = \frac{-c}{ad-bc} = \frac{-c}{|A|}, \qquad x_2 = \frac{-b}{ad-bc} = \frac{-b}{|A|}, \qquad y_2 = \frac{a}{ad-bc} = \frac{a}{|A|}$$

Conseqüentemente,

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{bmatrix} = \frac{1}{|A|}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Em outras palavras, quando $|A| \neq 0$, a inversa da matriz 2×2 A é obtida como a seguir:

(1) troque os elementos da diagonal principal;
(2) tome os negativos dos outros elementos;
(3) multiplique a matriz por $1/|A|$ ou, equivalentemente, divida cada elemento por $|A|$.

Por exemplo, se $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$, então $|A| = -2$ e, logo,

$$A^{-1} = \frac{1}{-2}\begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}$$

Por outro lado, se $|A| = 0$, não podemos resolver o sistema para as incógnitas x_1, y_1, x_2, y_2, e A^{-1} não existe. Embora não haja uma fórmula simples para matrizes de ordem maior, este resultado em geral é verdade.

Teorema 5-5: uma matriz A é inversível se e somente se tem determinante diferente de zero.

5.10 OPERAÇÕES ELEMENTARES NAS LINHAS E ELIMINAÇÃO DE GAUSS (OPCIONAL)

Esta seção discute o método de eliminação de Gauss no contexto de operações elementares entre as linhas.

Operações Elementares nas Linhas

Considere a matriz $A = [a_{ij}]$, cujas linhas serão denotadas, respectivamente, por R_1, R_2, ..., R_m. O primeiro elemento não nulo em uma linha R_i é dito o *pivô*[†]. Uma linha só de zeros é dita uma *linha zero*. Logo, uma linha zero não tem pivô.

As seguintes operações em A são chamadas de *operações elementares nas linhas*.

[$\mathbf{E}_1$] Troque a linha R_i pela linha R_j. Esta operação será indicada por: "troque R_i e R_j".

[$\mathbf{E}_2$] Multiplique cada elemento da linha R_i por uma constante não nula k. Esta operação será indicada por: "multiplique R_i por k".

[†] N. de T. No original, *leading*, termo cuja tradução literal é de uso raro em textos em português.

[$\mathbf{E}_3$] Adicione um múltiplo de uma linha R_i à outra linha R_j ou, em outras palavras, substitua R_j pela soma $kR_i + R_j$. Esta operação será indicada por : "some kR_i e R_j".

Para evitar frações, podemos efetuar [$\mathbf{E}_2$] e [$\mathbf{E}_3$] em uma etapa, isto é, podemos aplicar a operação seguinte:

[$\mathbf{E}$] Adicione um múltiplo de uma linha R_i a um múltiplo não nulo de outra linha R_j ou, em outras palavras, substitua R_j pela soma $kR_i + k'R_j$, onde $k' \neq 0$. Indicamos esta operação por: "some kR_i e $k'R_j$".

Enfatizamos que, nas operações nas linhas [$\mathbf{E}_3$] e [$\mathbf{E}$], apenas a linha R_j é de fato alterada.

Notação: As matrizes A e B são ditas *linha-equivalentes* (escreve-se $A \sim B$) se a matriz B pode ser obtida de A usando operações elementares nas linhas.

Matrizes Escalonadas

Uma matriz A é chamada *matriz escalonada*, ou dita estar em *forma escalonada*, se as duas condições seguintes ocorrem:

(i) Todas as linhas zero, se existir alguma, estão na parte inferior da matriz.

(ii) Cada pivô não nulo está à direita do pivô não nulo da linha precedente.

Diz-se que a matriz está na *forma canônica por linhas* se tem as seguintes propriedades adicionais:

(iii) Todo pivô não nulo é 1.

(iv) Cada pivô não nulo é o único elemento não nulo da sua coluna.

A matriz zero 0, com qualquer número de linhas ou colunas, é um exemplo especial de uma matriz na forma canônica por linhas. A matriz identidade n-quadrada I_n é outro exemplo de uma matriz na forma canônica por linhas.

Diz-se que uma matriz quadrada A está na *forma triangular* se os elementos da sua diagonal $a_{11}, a_{22}, \ldots, a_{nn}$ são os pivôs não nulos. Logo, uma matriz quadrada na forma triangular é um caso especial de uma matriz escalonada. A matriz identidade I é o único exemplo de matriz quadrada que está na forma triangular e na forma canônica por linhas.

Exemplo 5.11 As seguintes matrizes são matrizes escalonadas cujos elementos pivô foram circulados:

$$\begin{bmatrix} \textcircled{2} & 3 & 2 & 0 & 4 & 5 & -6 \\ 0 & 0 & \textcircled{1} & 1 & -3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \textcircled{6} & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} \textcircled{1} & 2 & 3 \\ 0 & 0 & \textcircled{1} \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \textcircled{1} & 3 & 0 & 0 & 4 \\ 0 & 0 & 0 & \textcircled{1} & 0 & -3 \\ 0 & 0 & 0 & 0 & \textcircled{1} & 2 \end{bmatrix}, \quad \begin{bmatrix} \textcircled{2} & 4 & 7 \\ 0 & \textcircled{5} & 8 \\ 0 & 0 & \textcircled{6} \end{bmatrix}$$

(Os zeros que precedem e ficam abaixo dos pivôs em uma matriz na forma escalonada formam um desenho padrão em forma de "escada", como indicado acima pelo sombreado.) A terceira matriz está na forma canônica por linhas, já que a terceira coluna contém um pivô não nulo e mais um elemento não nulo. A primeira matriz não está na forma canônica por linhas, já que alguns pivôs não nulos não valem 1. A última matriz está na forma triangular.

Eliminação Gaussiana na Forma Matricial

Considere uma matriz qualquer A. Dois algoritmos são descritos a seguir. O primeiro transforma a matriz A em uma matriz na forma escalonada (usando apenas operações elementares nas linhas), e o segundo algoritmo transforma a matriz escalonada em uma matriz na forma canônica por linhas. (Os dois algoritmos juntos são chamados de *eliminação de Gauss*).

Algoritmo 5.10A (**Eliminação à frente**) A entrada é uma matriz arbitrária $A = [a_{ij}]$.

Passo 1 Ache a primeira coluna com um elemento não nulo. Se não existir tal coluna, SAIA. (Temos a matriz zero.) Caso contrário, seja j_1 o índice desta coluna.

(a) Arranje de tal forma que $a_{1j_1} \neq 0$. Isto é, se necessário, troque a posição das linhas de tal forma que um elemento não nulo apareça na primeira linha na coluna j_1.

(b) Use a_{1j_1} como *pivô* para obter zeros abaixo de a_{1j_1}. Isto é, para $i>1$:

(1) Faça $m = -a_{ij_1}/a_{1j_1}$.

(2) Some mR_1 a R_i.

[Isso substitui a linha R_i por $-(a_{ij_1}/a_{1j_1})R_1 + R_i$.]

Passo 2 Repita o Passo 1 com a submatriz formada por todas as linhas, excluindo a primeira linha. Denotamos por j_2 a primeira coluna na submatriz com um elemento não nulo. Portanto, ao final do Passo 2, temos $a_{2j_2} \neq 0$.

Passo 3 a r + 1 Continue o processo acima até que a submatriz não tenha elementos não nulos.

Enfatizamos que, ao final do algoritmo, os elementos *pivô* serão

$$a_{1j_1}, a_{2j_2}, \ldots, a_{rj_r}$$

onde r denota o número de linhas não nulas da matriz escalonada.

Observação 1: O número no Passo 1(b),

$$m = -\frac{a_{i1}}{a_{j1}} = -\frac{\text{coeficiente a ser deletado}}{\text{pivô}}$$

é chamado *multiplicador*.

Observação 2: A operação no Passo 1 (b) pode ser substituída por

"Some $-a_{ij_1}R_1$ a $a_{1j_1}R_i$"

Isso evitaria frações se todos os escalares fossem originalmente inteiros.

Algoritmo 5.10B (**Eliminação para trás**): A matriz de entrada $A = [a_{ij}]$ está na forma escalonada com elementos pivô $a_{1j_1}, a_{2j_2}, \ldots a_{rj_r}$.

Passo 1 (a) Multiplique a última linha não nula R_r por $1/a_{rj_r}$, de tal maneira que o elemento pivô seja igual a 1.

(b) Use $a_{rj_r} = 1$ para obter zeros acima do pivô. Isto é, para $i = r-1, r-2, \ldots, 1$:

(1) Faça $m = -a_{ir_1}$.

(2) Some mR_r a R_i.

Em outras palavras, aplique a operação elementar entre as linhas

"Some $-a_{ir_1}R_r$ a R_i"

[Isso substitui a linha R_i por $-a_{ir_1}R_r + R_i$.]

Passo 2 a r – 1 Repita o Passo 1 para as linhas $R_{r-1}, R_{r-2}, \ldots, R_2$.

Passo r Multiplique R_1 por $1/a_{1j_1}$.

Exemplo 5.12 Ache a forma canônica por linhas de

$$A = \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 2 & 4 & -4 & 6 & 10 \\ 3 & 6 & -6 & 9 & 13 \end{bmatrix}.$$

Primeiramente reduza A à forma escalonada usando o Algoritmo 10.5A. Especificamente, use $a_{11} = 1$ como um pivô para obter zeros abaixo de a_{11}, isto é, aplique as operações sobre as linhas "Some $-2R_1$ a R_2" e "Some $-3R_1$ a R_3". Então use $a_{23} = 2$ como pivô para obter 0 abaixo de a_{23}, isto é, aplique a operação sobre linhas "Some $-\frac{3}{2}R_2$ a R_3". Obtém-se

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 3 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

A matriz A está agora na forma escalonada.

Agora use o Algoritmo 10.5B para reduzir A à forma canônica por linhas. Especificamente, multiplique R_3 por $-\frac{1}{2}$ de tal maneira que o pivô seja $a_{35} = 1$, e use $a_{35} = 1$ como pivô para obter zeros na parte superior com as operações: "Some $-6R_3$ a R_2" e "Some $-2R_3$ a R_1". Obtém-se:

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 2 \\ 0 & 0 & 2 & 4 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Multiplique R_2 por $\frac{1}{2}$ de tal maneira que o pivô $a_{23} = 1$, e então use $a_{23} = 1$ como pivô para obter 0 na parte superior pela operação "Some $3R_2$ a R_1". Obtém-se

$$A \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 7 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

A última matriz é a forma canônica por linhas de A.

Os Algoritmos 10.5A e 10.5B mostram que qualquer matriz é linha-equivalente a pelo menos uma matriz na forma canônica por linhas (chamada *forma canônica por linhas* de A).

Solução por Matrizes de Sistemas de Equações Lineares

Considere um sistema S de equações lineares ou, equivalentemente, uma equação matricial $AX = B$ com matriz aumentada $M = [A, B]$. O sistema é resolvido pela aplicação do algoritmo de eliminação Gaussiana a M como a seguir.

Parte A (*Redução*): Reduza a matriz aumentada M à forma escalonada. Se uma linha da forma $(0, 0, \ldots, 0, b)$, com $b \neq 0$, aparece, então *pare*. O sistema não tem solução.

Parte B (*Substituição para trás*): Reduza a matriz aumentada M à sua forma canônica por linhas.

A única solução do sistema ou, quando a solução não é única, a forma com variável livre da solução é facilmente obtida da forma canônica por linhas de M.

O exemplo seguinte aplica o algoritmo acima a um sistema S com solução única. Os casos em que S não tem solução e em que S tem infinitas soluções são mostrados no Problema 5.32 e 5.31, respectivamente.

Exemplo 5.13 Resolva o sistema:

$$\begin{aligned} x + 2y + z &= 3 \\ 2x + 5y - z &= -4 \\ 3x - 2y - z &= 5 \end{aligned}$$

Reduza a matriz aumentada M à forma escalonada e depois à forma canônica por linhas como a seguir.

$$M = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 5 & -1 & -4 \\ 3 & -2 & -1 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & -8 & -4 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & -28 & -84 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 2 & 1 & 3 \\ 0 & 1 & -3 & -10 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Portanto, o sistema tem a solução única $x = 2$, $y = -1$ e $z = 3$, ou, equivalentemente, o vetor $u = (2, -1, 3)$. Notamos que a forma escalonada da matriz M já indicava que a solução era única, uma vez que correspondia a um sistema triangular.

Inversa de uma Matriz $n \times n$

Considere uma matriz 3×3 arbitrária $A = [a_{ij}]$. Determinar $A^{-1} = [x_{ij}]$ se reduz a calcular a solução de três sistemas 3×3 de equações lineares. As matrizes aumentadas desses três sistemas são:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & 1 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 1 \\ a_{31} & a_{32} & a_{33} & 0 \end{bmatrix}, \quad \begin{bmatrix} a_{11} & a_{12} & a_{13} & 0 \\ a_{21} & a_{22} & a_{23} & 0 \\ a_{31} & a_{32} & a_{33} & 1 \end{bmatrix}.$$

Note que a matriz original A é a matriz dos coeficientes de todos os três sistemas. Note também que as três colunas de constantes formam a matriz identidade I. Esses três sistemas podem ser simultaneamente resolvidos pelo algoritmo seguinte, que vale para qualquer matriz $n \times n$.

Algoritmo 5.10 C Determina a inversa de uma matriz $n \times n$.

Passo 1 Forme a matriz $n \times 2n$ $M = [A, I]$; isto é, A está na metade esquerda de M, e a Matriz identidade I está na metade direita de M.

Passo 2 Reduza M por linhas à forma escalonada. Se o processo gerar uma linha zero na metade A de M, então *pare* (A não tem inversa). Caso contrário, a metade A está agora na forma triangular.

Passo 3 Reduza M à forma canônica por linhas.

$$M \sim [I, B]$$

onde I substituiu A na metade esquerda de M.

Passo 4 Faça $A^{-1} = B$, onde B é a matriz que está agora na metade direita de M.

Exemplo 5.14 Ache a inversa de

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{bmatrix}$$

Forme a matriz $M = (A, I)$ e reduza M à forma escalonada:

$$M = \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 2 & -1 & 3 & 0 & 1 & 0 \\ 4 & 1 & 8 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 1 & 0 & -4 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 1 & 0 & 0 \\ 0 & -1 & -1 & -2 & 1 & 0 \\ 0 & 0 & -1 & -6 & 1 & 1 \end{array}\right]$$

Na forma escalonada, a metade esquerda de M está na forma triangular; logo, A é inversível. Depois reduza M à sua forma canônica por linhas:

$$M \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & -1 & 0 & 4 & 0 & -1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -11 & 2 & 2 \\ 0 & 1 & 0 & -4 & 0 & 1 \\ 0 & 0 & 1 & 6 & -1 & -1 \end{array}\right]$$

A matriz identidade está na metade esquerda da matriz final; portanto, a metade direita é A^{-1}. Em outras palavras,

$$A^{-1} = \begin{bmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{bmatrix}$$

5.11 MATRIZES BOOLEANAS (ZERO – UM)

Os *dígitos binários*, ou *bits*, são os símbolos 0 e 1. Considere as operações seguintes com estes dígitos:

+	0	1
0	0	1
1	1	1

×	0	1
0	0	0
1	0	1

Entendendo esses dígitos como valores lógicos (0 representando FALSO e 1 representando VERDADEIRO), as operações acima correspondem, respectivamente, às operações lógicas OU ($\vee$) e E ($\wedge$); isto é,

$\vee$	F	V
F	F	V
V	V	V

$\wedge$	F	V
F	F	F
V	F	V

(As operações acima em 0 e 1 são chamadas de *operações booleanas*, uma vez que também correspondem às operações da álgebra booleana, discutida no Capítulo 15.)

Seja $A = [a_{ij}]$ uma matriz cujos elementos são os *bits* 0 e 1 sujeitos às operações booleanas definidas acima. Então A é chamada *matriz booleana*. O *produto booleano* de duas tais matrizes é o produto usual, exceto pelo fato de que agora usamos as operações booleanas de adição e multiplicação. Por exemplo, se

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \qquad \text{então} \qquad AB = \begin{bmatrix} 0+0 & 1+1 \\ 0+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Pode-se mostrar facilmente que, se A e B são matrizes booleanas, o produto booleano AB pode ser obtido calculando o produto usual de A e B e depois substituindo todo dígito não nulo por 1.

Problemas Resolvidos

Vetores

5.1 Seja $u = (2, -7, 1)$, $v = (-3, 0, 4)$ e $w = (0, 5, 8)$. Ache:

$$(a)\ u + v; \quad (b)\ v + w; \quad (c)\ -3u; \qquad (d)\ -w.$$

(*a*) Some os componentes correspondentes:

$$u + v = (2, -7, 1) + (-3, 0, 4) = (2 - 3, -7 + 0, 1 + 4) = (-1, -7, 5)$$

(*b*) Some os componentes correspondentes:

$$v + w = (-3, 0, 4) + (0, 5, -8) = (-3 + 0, 0 + 5, 4 - 8) = (-3, 5, -4)$$

(*c*) Multiplique cada componente de u pelo escalar –3.

$$-3u = -3(2, -7, 1) = (-6, 21, -3)$$

(*d*) Troque o sinal de cada componente ou, equivalentemente, multiplique cada componente por –1;

$$-w = -(0, 5, -8) = (0, -5, 8)$$

5.2 Sejam u, v e w os vetores do Problema 5.1. Ache: (*a*) $3u - 4v$; (*b*) $2u + 3v - 5w$.

Primeiramente efetue a multiplicação por escalar e depois a adição de vetores.

(*a*) $3u - 4v = 3(2, -7, 1) - 4(-3, 0, 4) = (6, -21, 3) + (12, 0, -16) = (18, -21, -13)$.

(*b*) $2u + 3v - 6w =$

$$2(2, -7, 1) + 3(-3, 0, 4) - 5(0, 5, -8) = (4, -14, 2) + (-9, 0, 12) + (0, -25, 40) = (-5, -39, 54).$$

5.3 Sejam u, v e w os vetores do Problema 5.1. Ache: (*a*) $u \cdot v$; (*b*) $u \cdot w$; (*c*) $v \cdot w$.

Multiplique os componentes correspondentes e então some.

(*a*) $u \cdot v = 2(-3) - 7(0) + 1(4) = -6 + 0 + 4 = -2$.

(*b*) $u \cdot w = 2(0) - 7(5) + 1(-8) = 0 - 35 - 8 = -43$.

(*c*) $v \cdot w = -3(0) + 0(5) + 4(-8) = 0 + 0 - 32 = -32$.

5.4 Ache $\|u\|$ onde: (*a*) $u = (3, -12, -4)$; (*b*) $u = (2, -3, 8, -7)$.

Primeiramente ache $\|u\|^2 = u \cdot u$ elevando os componentes ao quadrado e depois somando. Então, $\|u\| = \sqrt{\|u\|^2}$.

(*a*) $\|u\|^2 = (3)^2 + (-12)^2 + (-4)^2 = 9 + 144 + 16 = 169$.

Portanto, $\|u\| = \sqrt{169} = 13$.

(*b*) $\|u\|^2 = 4 + 9 + 64 + 49 = 126$. Portanto, $\|u\| = \sqrt{126}$.

5.5 Ache x e y se $x(1,1) + y(2,-1) = (1,4)$.

Primeiramente multiplique pelos escalares x e y e depois some.

$$x(1, 1) + y(2, -1) \quad = \quad (x, x) + (2y, -y) \quad = \quad (x + 2y, x - y) \quad = \quad (1, 4)$$

Dois vetores são iguais apenas quando seus componentes correspondentes são iguais; portanto, iguale os componentes correspondentes para obter $x + 2y = 1$ e $x - y = 4$. Finalmente resolva o sistema de equações para obter $x = 3$ e $y = -1$.

5.6 Suponha que $u = \begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix}$ e $w = \begin{bmatrix} 3 \\ -1 \\ -2 \end{bmatrix}$. Ache: (*a*) $5u - 2v$; (*b*) $-2u + 4v - 3w$.

(*a*) $5u - 2v = 5\begin{bmatrix} 5 \\ 3 \\ -4 \end{bmatrix} - 2\begin{bmatrix} -1 \\ 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 25 \\ 15 \\ -20 \end{bmatrix} + \begin{bmatrix} 2 \\ -10 \\ 4 \end{bmatrix} = \begin{bmatrix} 27 \\ 5 \\ -24 \end{bmatrix}$.

(*b*) $-2u + 4v - 3w = \begin{bmatrix} -10 \\ -6 \\ 8 \end{bmatrix} + \begin{bmatrix} -4 \\ 20 \\ 8 \end{bmatrix} + \begin{bmatrix} -9 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} -23 \\ 17 \\ 22 \end{bmatrix}$.

Adição de Matrizes e Multiplicação por Escalar

5.7 Dados $A = \begin{bmatrix} 1 & 2 & -3 \\ 4 & -5 & 6 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -5 \end{bmatrix}$. Ache: (*a*) $A + B$; (*b*) $3A$ e $-4B$.

(*a*) Ache os elementos correspondentes:

$$A + B = \begin{bmatrix} 1+1 & 2+(-1) & -3+2 \\ 4+0 & -5+3 & 6+(-5) \end{bmatrix} = \begin{bmatrix} 2 & 1 & -1 \\ 4 & -2 & 1 \end{bmatrix}$$

(*b*) Multiplique cada elemento pelo escalar dado.

$$3A = \begin{bmatrix} 3(1) & 3(2) & 3(-3) \\ 3(4) & 3(-5) & 3(6) \end{bmatrix} = \begin{bmatrix} 3 & 6 & -9 \\ 12 & -15 & 18 \end{bmatrix}$$

$$-4B = \begin{bmatrix} -4(1) & -4(-1) & -4(2) \\ -4(0) & -4(3) & -4(-5) \end{bmatrix} = \begin{bmatrix} -4 & 4 & -8 \\ 0 & -12 & 20 \end{bmatrix}$$

5.8 Ache $2A - 3B$, onde $A = \begin{bmatrix} 1 & -2 & 3 \\ 4 & 5 & -6 \end{bmatrix}$ e $B = \begin{bmatrix} 3 & 0 & 2 \\ -7 & 1 & 8 \end{bmatrix}$.

Primeiramente efetue a multiplicação por escalar e depois a adição de matrizes.

$$2A - 3B = \begin{bmatrix} 2 & -4 & 6 \\ 8 & 10 & -12 \end{bmatrix} + \begin{bmatrix} -9 & 0 & -6 \\ 21 & -3 & -24 \end{bmatrix} = \begin{bmatrix} -7 & -4 & 0 \\ 29 & 7 & -36 \end{bmatrix}$$

(Note que multiplicamos B por –3 e depois somamos, no lugar de multiplicar B por 3 e depois subtrairmos. Em geral, isso evita erros.)

5.9 Ache x, y, z, t, onde $3\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} x & 6 \\ -1 & 2t \end{bmatrix} + \begin{bmatrix} 4 & x+y \\ z+t & 3 \end{bmatrix}$.

Primeiramente escreva cada lado como uma única matriz:

$$\begin{bmatrix} 3x & 3y \\ 3z & 3t \end{bmatrix} = \begin{bmatrix} x+4 & x+y+6 \\ z+t-1 & 2t+3 \end{bmatrix}$$

Iguale os elementos correspondentes para obter um sistema de quatro equações.

$$\begin{aligned} 3x &= x + 4 \\ 3y &= x + y + 6 \\ 3z &= z + t - 1 \\ 3t &= 2t + 3 \end{aligned} \quad \text{ou} \quad \begin{aligned} 2x &= 4 \\ 2y &= 6 + x \\ 2z &= t - 1 \\ t &= 3 \end{aligned}$$

A solução é $x = 2, y = 4, z = 1, t = 3$.

5.10 Prove o Teorema 5.1(v): $k(A + B) = kA + kB$.

Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$. Então, o elemento ij de $A + B$ é $a_{ij} + b_{ij}$. Portanto, $k(a_{ij} + b_{ij})$ é o elemento ij de $k(A + B)$. Por outro lado, os elementos ij de kA e kB são ka_{ij} e kb_{ij}, respectivamente. Portanto, $ka_{ij} + kb_{ij}$ é o elemento ij. Entretanto, para escalares, $k(a_{ij} + b_{ij}) = ka_{ij} + kb_{ij}$. Logo, $k(A + B)$ e $kA + kB$ têm os mesmos elementos ij. Portanto, $k(A + B) = kA + kB$.

Multiplicação de Matrizes

5.11 Calcule: (*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix}$; (*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix}$.

Multiplique os elementos correspondentes e então some.

(*a*) $[3, -2, 5]\begin{bmatrix} 6 \\ 1 \\ -4 \end{bmatrix} = 3(6) - 2(1) + 5(-4) = 18 - 2 - 20 = -4.$

(*b*) $[2, -1, 7, 4]\begin{bmatrix} 5 \\ -3 \\ -6 \\ 9 \end{bmatrix} = 10 + 3 - 42 + 36 = 7.$

5.12 Denote por $(r \times s)$ uma matriz $r \times s$. Ache a dimensão das matrizes produto definidas:

(*a*) $(2 \times 3)(3 \times 4)$ (*c*) $(1 \times 2)(3 \times 1)$ (*e*) $(4 \times 4)(3 \times 3)$
(*b*) $(4 \times 1)(1 \times 2)$ (*d*) $(5 \times 2)(2 \times 3)$ (*f*) $(2 \times 2)(2 \times 4)$

Em cada caso, o produto é definido se os números internos são iguais, e então o produto terá a dimensão dos números externos na ordem dada.

(*a*) 2×4 (*c*) Não definido (*e*) Não definido
(*b*) 4×2 (*d*) 5×3 (*f*) 2×4

5.13 Sejam $A = \begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix}$. Ache: (*a*) AB; (*b*) BA.

(*a*) Como A é 2×2 e B é 2×3, o produto AB é definido e é uma matriz 2×3. Para obter a primeira linha de AB, multiplique a primeira linha $[1, 3]$ de A pelas colunas $\begin{bmatrix} 2 \\ 3 \end{bmatrix}$, $\begin{bmatrix} 0 \\ -2 \end{bmatrix}$, $\begin{bmatrix} -4 \\ 6 \end{bmatrix}$ de B, respectivamente :

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 1(2) + 3(3) & 1(0) + 3(-1) & 1(-4) + 3(6) \\ & & \end{bmatrix}$$
$$= \begin{bmatrix} 2 + 9 & 0 - 6 & -4 + 18 \\ & & \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ & & \end{bmatrix}$$

Para obter os elementos da segunda linha de AB, multiplique a segunda linha $[2, -1]$ de A pelas colunas de B, respectivamente:

$$\begin{bmatrix} 1 & 3 \\ 2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 0 & -4 \\ 3 & -2 & 6 \end{bmatrix} = \begin{bmatrix} 11 & -6 & 14 \\ 4 - 3 & 0 + 2 & -8 - 6 \end{bmatrix}$$

Portanto
$$AB = \begin{bmatrix} 11 & -6 & 14 \\ 1 & 2 & -14 \end{bmatrix}$$

(*b*) Note que B é 2×3 e A é 2×2. Como os números internos, 3 e 2, não são iguais, o produto BA não é definido.

5.14 Compute: (*a*) $\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 2 & -1 \end{bmatrix}$; (*b*) $\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ -7 \end{bmatrix}$; (*c*) $\begin{bmatrix} 1 \\ -6 \end{bmatrix}\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}$; (*d*) $\begin{bmatrix} 1 \\ 6 \end{bmatrix}[3, 2]$;
(*e*) $[2, -1]\begin{bmatrix} 1 \\ -6 \end{bmatrix}$.

(*a*) O primeiro fator é 2×2, e o segundo é 2×2; logo, o produto é definido e é uma matriz 2×2:

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 4 + 12 & 0 + 12 \\ -12 + 10 & 0 - 5 \end{bmatrix} = \begin{bmatrix} 16 & -6 \\ -2 & -5 \end{bmatrix}$$

(*b*) O primeiro fator é 2×2, e o segundo é 2×1; logo, o produto é definido e é uma matriz 2×1:

$$\begin{bmatrix} 1 & 6 \\ -3 & 5 \end{bmatrix}\begin{bmatrix} 2 \\ -7 \end{bmatrix} = \begin{bmatrix} 2-42 \\ -6-35 \end{bmatrix} = \begin{bmatrix} -40 \\ -41 \end{bmatrix}$$

(*c*) O primeiro fator é 2×1, e o segundo é 2×2. Como os números internos, 1 e 2, são diferentes, o produto não é definido.

(*d*) Aqui o primeiro fator é 2×1, e o segundo é 1×2; logo, o produto é definido e é uma matriz 2×2:

$$\begin{bmatrix} 1 \\ 6 \end{bmatrix}[3, 2] = \begin{bmatrix} 1(3) & 1(2) \\ 6(3) & 6(2) \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 18 & 12 \end{bmatrix}$$

(*e*) O primeiro fator é 1×2, e o segundo é 2×1; logo, o produto é definido como uma matriz 1×1, que escrevemos, tipicamente, como um escalar:

$$[2, -1]\begin{bmatrix} 1 \\ -6 \end{bmatrix} = 2(1) - 1(-6) = 2 + 6 = 8$$

5.15 Prove o Teorema 5.2(i): $(AB)C = A(BC)$.

Sejam $A = [a_{ij}]$, $B = [b_{jk}]$ e $C = [c_{kl}]$. Além disto, sejam $AB = S = [s_{ik}]$ e $BC = T = [t_{jl}]$.

Então,

$$s_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{im}b_{mk} = \sum_{j=1}^{m} a_{ij}b_{jk}$$

$$t_{jl} = b_{j1}c_{1l} + b_{j2}c_{2l} + \cdots + b_{jn}c_{nl} = \sum_{k=1}^{n} b_{jk}c_{kl}$$

Agora, multiplicando S por C, i.e., (AB) por C, o elemento na i-ésima linha e j-ésima coluna da matriz $(AB)C$ é

$$s_{i1}c_{1l} + s_{i2}c_{2l} + \cdots + s_{in}c_{nl} = \sum_{k=1}^{n} s_{ik}c_{kl} = \sum_{k=1}^{n}\sum_{j=1}^{m}(a_{ij}b_{jk})c_{kl}$$

Por outro lado, multiplicando A por T, i.e., AB por BC, o elemento na i-ésima linha e j-ésima coluna da matriz $A(BC)$ é

$$a_{i1}t_{1l} + a_{i2}t_{2l} + \cdots + a_{im}t_{ml} = \sum_{j=1}^{m} a_{ij}t_{jl} = \sum_{k=1}^{m}\sum_{j=1}^{n} a_{ij}(b_{jk}c_{kl})$$

Como as somas acima são iguais, o teorema está provado.

Transposta

5.16 Ache a transposta de cada matriz:

$$A = \begin{bmatrix} 1 & -2 & 3 \\ 7 & 8 & -9 \end{bmatrix}; \qquad B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}; \qquad C = [1, -3, 5, -7]; \qquad D = \begin{bmatrix} 2 \\ -4 \\ 6 \end{bmatrix}.$$

Reescreva as linhas de cada matriz como colunas para obter as transpostas das matrizes:

$$A^T = \begin{bmatrix} 1 & 7 \\ -2 & 8 \\ 3 & -9 \end{bmatrix}, \qquad B^T = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix}, \qquad C^T = \begin{bmatrix} 1 \\ -3 \\ 5 \\ -7 \end{bmatrix}, \qquad D^T = [2, -4, 6]$$

(Note que $B^T = B$; uma tal matriz é dita *simétrica*. Note também que a transposta do vetor linha C é um vetor coluna, e a transposta do vetor coluna D é um vetor linha.)

5.17 Seja $A = \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix}$. Ache: (*a*) AA^T; (*b*) A^TA.

Para obter A^T, reescreva as linhas de A como colunas: $A^T = \begin{bmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 4 \end{bmatrix}$. Então,

$$(a) \quad AA^T = \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 1+4+0 & 3-2+0 \\ 3-2+0 & 9+1+16 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 1 & 26 \end{bmatrix}.$$

$$(b) \quad A^TA = \begin{bmatrix} 1 & 3 \\ 2 & -1 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \\ 3 & -1 & 4 \end{bmatrix} = \begin{bmatrix} 1+9 & 2-3 & 0+12 \\ 2-3 & 4+1 & 0-4 \\ 0+12 & 0-4 & 0+16 \end{bmatrix} = \begin{bmatrix} 10 & -1 & 12 \\ -1 & 5 & -4 \\ 12 & -4 & 16 \end{bmatrix}.$$

5.18 Prove o Teorema 5.3(iii): $(AB)^T = B^TA^T$.

Suponha que $A = [a_{ik}]$ e $B = [b_{kj}]$. Então, o elemento ij de AB é

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj}$$

Portanto, (1) é o elemento ji (ordem reversa) de $(AB)^T$.

Por outro lado, a coluna j de B torna-se a linha j de B^T e a linha i de A torna-se coluna i de A^T. Conseqüentemente, o elemento ij de B^TA^T é

$$[b_{1j}, b_{2j}, \cdots, b_{mj}] \begin{bmatrix} a_{i1} \\ a_{i2} \\ \cdots \\ a_{im} \end{bmatrix} = b_{1j}a_{i1} + b_{2j}a_{i2} + \cdots + b_{mj}a_{im}$$

Portanto, $(AB)^T = B^TA^T$, já que os elementos correspondentes são iguais.

Matrizes Quadradas

5.19 Ache a diagonal de cada uma das matrizes seguintes:

$$(a)\ A = \begin{bmatrix} 1 & 3 & 6 \\ 2 & -5 & 8 \\ 4 & -2 & 7 \end{bmatrix}; \qquad (b)\ B = \begin{bmatrix} t-2 & 3 \\ -4 & t+5 \end{bmatrix}; \qquad (c)\ C = \begin{bmatrix} 1 & 2 & -3 \\ 4 & -5 & 6 \end{bmatrix}.$$

(*a*) A diagonal consiste nos elementos do canto superior esquerdo ao canto inferior direito da matriz, isto é, os elementos a_{11}, a_{22} e a_{33}. Portanto, a diagonal consiste nos escalares 1, – 5 e 7.

(*b*) A diagonal consiste no par $[t - 2t, t + 5]$.

(*c*) A diagonal é definida apenas para matrizes quadradas.

5.20 Seja $A = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}$. Ache: (*a*) A^2; (*b*) A^3.

$$(a) \quad A^2 = AA = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} = \begin{bmatrix} 1+8 & 2-6 \\ 4-12 & 8+9 \end{bmatrix} = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix}.$$

$$(b) \quad A^3 = AA^2 = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} = \begin{bmatrix} 9-16 & -4+34 \\ 36+24 & -16-51 \end{bmatrix} = \begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix}.$$

5.21 Sejam $f(x) = 2x^3 - 4x + 5$ e $g(x) = x^2 + 2x - 11$. Para a matriz A do Problema 5.20, ache: (a) $f(A)$; (b) $g(A)$.

(a) Compute $f(a)$ primeiramente substituindo x por A e $5I$ no termo constante 5 em $f(x) = 2x^3 - 4x + 5$:

$$f(A) = 2A^3 - 4A + 5I = 2\begin{bmatrix} -7 & 30 \\ 60 & -67 \end{bmatrix} - 4\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Então multiplique cada matriz pelo seu respectivo escalar:

$$f(A) = \begin{bmatrix} -14 & 60 \\ 120 & -134 \end{bmatrix} + \begin{bmatrix} -4 & -8 \\ -16 & 12 \end{bmatrix} + \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$$

Finalmente, some os elementos correspondentes nas matrizes:

$$f(A) = \begin{bmatrix} -14 - 4 + 5 & 60 - 8 + 0 \\ 120 - 16 + 0 & -134 + 12 + 5 \end{bmatrix} = \begin{bmatrix} -13 & 52 \\ 104 & -117 \end{bmatrix}$$

(b) Compute $g(a)$ primeiramente substituindo x por A e $11I$ no termo constante 11 em $g(x) = x^2 + 2x - 11$:

$$g(A) = A^2 + 2A - 11I = \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + 2\begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix} - 11\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 9 & -4 \\ -8 & 17 \end{bmatrix} + \begin{bmatrix} 2 & 4 \\ 8 & -6 \end{bmatrix} + \begin{bmatrix} -11 & 0 \\ 0 & -11 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

(Como $g(A) = 0$, a matriz A é um zero do polinômio $g(x)$.)

Determinantes e Inversas

5.22 Compute o determinante de cada matriz:

$$(a)\ \begin{bmatrix} 4 & 5 \\ -3 & -2 \end{bmatrix}; \quad (b)\ \begin{bmatrix} -2 & 7 \\ 0 & 6 \end{bmatrix}; \quad (c)\ \begin{bmatrix} a-b & b \\ b & a+b \end{bmatrix}; \quad (d)\ \begin{bmatrix} a-b & a \\ a & a+b \end{bmatrix}.$$

Use a fórmula $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$ para obter:

(a) $\begin{vmatrix} 4 & 5 \\ -3 & -2 \end{vmatrix} = 4(-2) - 5(-3) = -8 + 15 = 7.$

(b) $\begin{vmatrix} -2 & 7 \\ 0 & 6 \end{vmatrix} = -2(6) - 7(0) = -12 + 0 = -12.$

(c) $\begin{vmatrix} a-b & b \\ b & a+b \end{vmatrix} = (a-b)(a+b) - b^2 = a^2 - b^2 - b^2 = a^2 - 2b^2.$

(d) $\begin{vmatrix} a-b & a \\ a & a+b \end{vmatrix} = (a-b)(a+b) - a^2 = a^2 - b^2 - a^2 = -b^2.$

5.23 Ache o determinante de cada matriz:

$$(a)\ \begin{bmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{bmatrix}; \quad (b)\ \begin{bmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{bmatrix}; \quad (c)\ \begin{bmatrix} 2 & -3 & 4 \\ 1 & 2 & -3 \\ -1 & -2 & 5 \end{bmatrix}.$$

(*Sugestão:* use o diagrama da Seção 5.9.)

$$(a)\quad \begin{vmatrix} 1 & 2 & 3 \\ 4 & -2 & 3 \\ 0 & 5 & -1 \end{vmatrix} = 2 + 0 + 60 - 0 - 15 + 8 = 55.$$

$$(b)\quad \begin{vmatrix} 4 & -1 & -2 \\ 0 & 2 & -3 \\ 5 & 2 & 1 \end{vmatrix} = 8 + 15 + 0 + 20 + 24 + 0 = 67.$$

$$(c)\quad \begin{vmatrix} 2 & -3 & 4 \\ 1 & 2 & -3 \\ -1 & -2 & 5 \end{vmatrix} = 20 - 9 - 8 + 8 - 12 + 15 = 14.$$

5.24 Ache a inversa, se possível, de cada matriz:

$$(a)\ A = \begin{bmatrix} 5 & 3 \\ 4 & 2 \end{bmatrix}; \qquad (b)\ B = \begin{bmatrix} 2 & -3 \\ 1 & 3 \end{bmatrix}; \qquad (c)\ C = \begin{bmatrix} -2 & 6 \\ 3 & -9 \end{bmatrix}.$$

Para uma matriz 2×2, use a fórmula desenvolvida na Seção 5.9.

(*a*) Primeiramente ache $|A| = 5(2) - 3(4) = 10 - 12 = -2$. Depois, troque a posição dos elementos da diagonal, tome os negativos dos elementos na antidiagonal e multiplique por $1/|A|$:

$$A^{-1} = -\frac{1}{2}\begin{bmatrix} 2 & -3 \\ -4 & 5 \end{bmatrix} = \begin{bmatrix} -1 & \frac{3}{2} \\ 2 & -\frac{5}{2} \end{bmatrix}$$

(*b*) Primeiramente ache $|B| = 2(3) - (-3)(1) = 6 + 3 = 9$. Depois, troque a posição dos elementos da diagonal, tome os negativos dos elementos na antidiagonal e multiplique por $1/|B|$:

$$B^{-1} = \frac{1}{9}\begin{bmatrix} 3 & 3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ -\frac{1}{9} & \frac{2}{9} \end{bmatrix}$$

(*c*) Primeiramente ache $|C| = -2(-9) - 6(3) = 18 - 18 = 0$. Como $|C| = 0$, C não tem inversa.

5.25 Ache a inversa de $A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -3 & 6 \\ 1 & 1 & 7 \end{bmatrix}$.

Forme a matriz $M = (A, I)$ e reduza M por linhas para a forma escalonada:

$$M = \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 2 & -3 & 6 & 0 & 1 & 0 \\ 1 & 1 & 7 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 3 & 5 & -1 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & -2 & 1 & 0 \\ 0 & 0 & -1 & 5 & -3 & 1 \end{array}\right]$$

Na forma escalonada, a metade esquerda de M está na forma triangular; portanto, A tem inversa. Agora reduza M por linhas à forma canônica:

$$M \sim \left[\begin{array}{ccc|ccc} 1 & -2 & 0 & 11 & -6 & 2 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 27 & -16 & 1 \\ 0 & 1 & 0 & 8 & -5 & 2 \\ 0 & 0 & 1 & -5 & 3 & -1 \end{array}\right]$$

A matriz final tem a forma $[I, A^{-1}]$; isto é, A^{-1} é a metade direita da última matriz. Portanto,

$$A^{-1} = \begin{bmatrix} 27 & -16 & 6 \\ 8 & -5 & 2 \\ -5 & 3 & -1 \end{bmatrix}$$

5.26 Ache a inversa de $B = \begin{bmatrix} 1 & 3 & -4 \\ 1 & 5 & -1 \\ 3 & 13 & -6 \end{bmatrix}$.

Forme a matriz $M = [B, I]$ e reduza M por linhas à forma escalonada:

$$M = \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 1 & 5 & -1 & 0 & 1 & 0 \\ 3 & 13 & -6 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 4 & 6 & -3 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 2 & 3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -2 & 1 \end{array}\right]$$

Na forma escalonada, M tem uma linha zero na sua metade esquerda; isto é, B não é redutível por linhas à forma triangular. Conseqüentemente, B não tem inversa.

5.27 Seja A uma matriz inversível com inversa B. Em outras palavras, $AB = BA = I$. Mostre que a matriz inversa B é única.

Sejam B_1 e B_2 duas inversas da matriz A. Em outras palavras, $AB_1 = B_1A = I$ e $AB_2 = B_2A = I$. Então, $B_1 = B_1I = B_1(AB_2) = (B_1A)B_2 = IB_2 = B_2$.

5.28 Suponha que A e B são matrizes inversíveis de mesma ordem. Mostre que AB é inversível e que $(AB)^{-1} = B^{-1}A^{-1}$.

Temos

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

e

$$(B^{-1}A^{-1}(AB) = B^{-1}(A^{-1}A)B = B^{-1}IB = B^{-1}B = I$$

Portanto, $B^{-1}A^{-1}$ é a inversa de AB; isto é, $(AB)^{-1} = B^{-1}A^{-1}$.

Matrizes Escalonadas, Redução por Linhas, Eliminação Gaussiana

5.29 Troque a posição das linhas de cada matriz para obter uma matriz escalonada:

$$(a)\ \begin{bmatrix} 0 & 1 & -3 & 4 & 6 \\ 4 & 0 & 2 & 5 & -3 \\ 0 & 0 & 7 & -2 & 8 \end{bmatrix}; \quad (b)\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 5 & -4 & 7 \end{bmatrix}; \quad (c)\ \begin{bmatrix} 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(*a*) Troque a primeira e a segunda linhas.

(*b*) Leve a linha zero para a parte inferior da matriz.

(*c*) Nenhuma troca de linhas pode levar a uma matriz escalonada.

5.30 Reduza por linhas a matriz seguinte à forma escalonada:

$$A = \begin{bmatrix} 1 & 2 & -3 & 0 \\ 2 & 4 & -2 & 2 \\ 3 & 6 & -4 & 3 \end{bmatrix}$$

Use a_{11} como pivô para obter zeros abaixo de a_{11}; isto é, aplique a operação entre as linhas "Some $-2R_1$ a R_2" e "Some $-3R_1$ a R_3". Isso leva à matriz

$$\begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 5 & 3 \end{bmatrix}$$

Agora use $a_{23} = 4$ como pivô para obter um zero abaixo de a_{23}; isto é, aplique a operação sobre as linhas "Some $-5R_2$ a $4R_3$" para obter a matriz

$$\begin{bmatrix} 1 & 2 & -3 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

que está na forma escalonada.

5.31 Quais das seguintes matrizes escalonadas estão na forma canônica por linhas?

$$\begin{bmatrix} 1 & 2 & -3 & 0 & 1 \\ 0 & 0 & 5 & 2 & -4 \\ 0 & 0 & 0 & 7 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 7 & -5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 5 & 0 & 2 \\ 0 & 1 & 2 & 0 & 4 \\ 0 & 0 & 0 & 1 & 7 \end{bmatrix}$$

A primeira matriz não está na forma canônica por linhas já que, por exemplo, dois dos pivôs não-nulos são 5 e 7, e não 1. Além disso, há um elemento não-nulo acima dos pivôs não nulos 5 e 7. A segunda e a terceira matrizes estão na forma canônica por linhas.

5.32 Reduza a seguinte matriz à forma canônica por linhas:

$$A = \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 1 & 1 & 4 & -1 & 3 \\ 2 & 5 & 9 & -2 & 8 \end{bmatrix}$$

Primeiramente reduza A à forma escalonada aplicando as operações "Some $-R_1$ a R_2" e "Some $-2R_1$ a R_3", e então a operação "Some $-3R_2$ a R_3". Essas operações levam à

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 9 & 3 & -4 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 2 & 1 \end{bmatrix}$$

Agora use a substituição para trás na matriz escalonada para obter a forma canônica por linhas de A. Especificamente, em primeiro lugar multiplique R_3 por $\frac{1}{2}$ para obter o pivô $a_{34} = 1$, então aplique as operações "Some $2R_3$ a R_2" e "Some $-R_3$ a R_1". Essas operações levam a

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 1 & 2 \\ 0 & 3 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 3 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Agora multiplique R_2 por $\frac{1}{3}$ tornando o pivô $a_{22} = 1$, e então aplique a operação "Some $2R_2$ a R_1". Obtemos

$$A \sim \begin{bmatrix} 1 & -2 & 3 & 0 & \frac{3}{2} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \frac{11}{3} & 0 & \frac{17}{6} \\ 0 & 1 & \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{bmatrix}$$

Já que $a_{11} = 1$, a última matriz é a forma canônica por linhas de A, como desejado.

5.33 Resolva o sistema seguinte usando a matriz aumentada M:

$$\begin{aligned} x + 3y - 2z + t &= 3 \\ 2x + 6y - 5z - 3t &= 7 \end{aligned}$$

Reduza a matriz aumentada M à forma escalonada e depois à forma canônica por linhas:

$$M = \begin{bmatrix} 1 & 3 & -2 & 1 & 3 \\ 2 & 6 & -5 & -3 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & -2 & 1 & 3 \\ 0 & 0 & 1 & -5 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 0 & -9 & 5 \\ 0 & 0 & 1 & -5 & 1 \end{bmatrix}$$

Escreva o sistema correspondente à forma canônica por linhas de M, isto é,

$$\begin{aligned} x + 3y \qquad & - 9t = 5 \\ & z - 5t = 1 \end{aligned}$$

As incógnitas x e z, que aparecem mais à esquerda na forma escalonada do sistema, são chamadas *variáveis básicas*, e as incógnitas remanescentes y e t são chamadas *variáveis livres*. Transfira as variáveis livres para o outro lado para obter a solução em função das variáveis livres[†]:

$$\begin{aligned} x &= 5 - 3y + 9t \\ z &= 1 + 5t \end{aligned}$$

A forma *paramétrica* da solução pode ser obtida tomando as variáveis livres como parâmetros, por exemplo, $y = a$ e $t = b$. Esse processo permite concluir

$$x = 5 - 3a + 9t, \qquad y = a, \qquad z = 1 + 5b, \qquad t = b \qquad \text{ou} \qquad u = (5 - 3a + 9t,\ a,\ 1 + 5b,\ b)$$

(que é uma outra forma da solução).

Uma solução particular do sistema pode ser agora obtida pela associação de valores às variáveis livres (ou parâmetros) e resolvendo para as variáveis básicas usando a forma em variáveis livres (ou paramétrica) da solução. Por exemplo, fazendo $y = 2$ e $t = 3$, obtemos $x = 26$ e $z = 16$. Portanto,

$$x = 26, \qquad y = 2, \qquad z = 16, \qquad t = 3 \qquad \text{ou} \qquad u = (26, 2, 16, 3)$$

é uma solução particular do sistema.

5.34 Resolva o sistema seguinte usando a matriz aumentada M:

$$\begin{aligned} x + \ \ y - 2z + 4t &= 5 \\ 2x + 2y - 3z + \ \ t &= 4 \\ 3x + 3y - 4z - 2t &= 3 \end{aligned}$$

Reduza a matriz aumentada M à forma escalonada e depois à forma canônica por linhas:

$$M = \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 2 & 2 & -3 & 1 & 4 \\ 3 & 3 & -4 & -2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 & 5 \\ 0 & 0 & 1 & -7 & -6 \\ \cancel{0} & \cancel{0} & \cancel{2} & \cancel{-14} & \cancel{-12} \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & -10 & -7 \\ 0 & 0 & 1 & -7 & -6 \end{bmatrix}$$

(A terceira linha da matriz é excluída, uma vez que é múltipla da segunda e resultará em uma linha nula.)

Escreva o sistema correspondente à forma canônica por linhas de M e então transfira as variáveis livres para o outro lado para obter a solução em função das variáveis livres:

$$\begin{aligned} x + y \qquad & - 10t = -7 \\ & z - \ 7t = -6 \end{aligned} \qquad \text{e então} \qquad \begin{aligned} x &= -7 - y + 10t \\ z &= -6 + 7t \end{aligned}$$

Aqui, x e z são as variáveis básicas, e y e t são as variáveis livres.

5.35 Resolva o sistema seguinte usando a matriz aumentada M:

$$\begin{aligned} x - 2y + 4z &= 2 \\ 2x - 3y + 5z &= 3 \\ 3x - 4y + 6z &= 7 \end{aligned}$$

Primeiramente reduza por linhas a matriz aumentada M à forma escalonada:

$$M = \begin{bmatrix} 1 & -2 & 4 & 2 \\ 2 & -3 & 5 & 3 \\ 3 & -4 & 6 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 2 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 4 & 2 \\ 0 & 1 & -3 & -1 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

[†] N. de T. No original, *free-variable form*.

Na forma escalonada, a terceira linha corresponde à equação degenerada

$$0x + 0y + 0z = 3$$

Portanto, o sistema não tem solução. (Note que a forma escalonada indica se o sistema tem ou não solução.)

Problemas Variados

5.36 Sejam $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ matrizes booleanas. Ache os produtos booleanos AB, BA e A^2.

Ache a matriz produto usual e substitua qualquer escalar não-nulo por 1. Portanto:

$$AB = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}; \qquad BA = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \qquad A^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

5.37 Seja $A = \begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix}$. (*a*) Ache um vetor coluna não nulo $u = \begin{bmatrix} x \\ y \end{bmatrix}$ tal que $Au = 3u$. (*b*) Descreva todos os vetores que satisfazem o item anterior.

(*a*) Monte primeiramente a equação na forma matricial $Au = 3u$ e depois escreva cada lado como uma única matriz (vetores coluna);

$$\begin{bmatrix} 1 & 3 \\ 4 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 3 \begin{bmatrix} x \\ y \end{bmatrix} \qquad \text{e} \qquad \begin{bmatrix} x + 3y \\ 4x - 3y \end{bmatrix} = \begin{bmatrix} 3x \\ 3y \end{bmatrix}$$

Iguale os elementos correspondentes para obter um sistema de equações e reduza o sistema à forma escalonada.

$$\begin{matrix} x + 3y = 3x \\ 4x - 3y = 3y \end{matrix} \quad \text{ou} \quad \begin{matrix} 2x - 3y = 0 \\ 4x - 6y = 0 \end{matrix} \quad \text{para} \quad \begin{matrix} 2x - 3y = 0 \\ 0 = 0 \end{matrix} \quad \text{ou} \quad 2x - 3y = 0$$

O sistema se reduz a uma equação linear (não degenerada) com duas incógnitas e, portanto, tem um número infinito de soluções. Para obter uma solução não nula, tome, por exemplo, $y = 2$; então, $x = 3$. Logo, $u = [3, 2]^T$ é uma solução não nula, como desejado.

(*b*) Para achar a solução geral, faça $y = a$, onde a é um parâmetro. Substitua $y = a$ em $2x - 3y = 0$ para obter $x = 3a/2$. Logo, $u = [3a/2, a]^T$ representa todas as soluções em questão.

Problemas Complementares

Vetores

5.38 Sejam $u = (1, -2, 4)$, $v = (3, 5, 1)$ e $w = (2, 1, -3)$. Ache: (*a*) $3u - 2v$; (*b*) $4u - v - 3w$; (*c*) $5u + 7v - 2w$.

5.39 Para os vetores no Problema 5.38, ache:

(*a*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*b*) $\|u\|$, $\|v\|$, $\|w\|$.

5.40 Sejam $u = (2, -1, 0, -3)$, $v = (1, -1, -1, 3)$ e $w = (1, 3, -2, 2)$. Ache: (*a*) $2u - 3v$; (*b*) $5u - 3v - 4w$; (*c*) $-u + 2v - 2w$; (*d*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*e*) $\|u\|$, $\|v\|$, $\|w\|$.

5.41 Sejam $u = \begin{bmatrix} 1 \\ 3 \\ -4 \end{bmatrix}$, $v = \begin{bmatrix} 2 \\ 1 \\ 5 \end{bmatrix}$ e $w = \begin{bmatrix} 3 \\ -2 \\ 6 \end{bmatrix}$. Ache: (*a*) $5u - 3v$; (*b*) $2u + 4v - 6w$; (*c*) $u \cdot v$, $u \cdot w$, $v \cdot w$; (*d*) $\|u\|$, $\|v\|$, $\|w\|$.

5.42 Ache x e y, onde: (*a*) $x(2,5) + y(4,-3) = (8,33)$; (*b*) $x(1,4) + y(2,-5) = (7,2)$.

5.43 Ache x, y, z, onde: $x\begin{bmatrix}1\\2\\3\end{bmatrix} + y\begin{bmatrix}2\\5\\-1\end{bmatrix} + z\begin{bmatrix}4\\-2\\3\end{bmatrix} = \begin{bmatrix}9\\-3\\16\end{bmatrix}$.

Operações entre Matrizes

Os problemas 5.44 a 5.58 se referem às seguintes matrizes:

$$A = \begin{bmatrix}1 & 2\\3 & -4\end{bmatrix}, \quad B = \begin{bmatrix}5 & 0\\-6 & 7\end{bmatrix}; \quad C = \begin{bmatrix}1 & -3 & 4\\2 & 6 & -5\end{bmatrix}; \quad D = \begin{bmatrix}3 & 7 & -1\\4 & -8 & 9\end{bmatrix}$$

5.44 Ache (*a*) $5A - 2B$; (*b*) $C + D$; (*c*) $2C - 3D$.

5.45 Ache (*a*) AB; (*b*) BA.

5.46 Ache (*a*) AC; (*b*) AD; (*c*) BC; (*d*) BD.

5.47 Ache (*a*) A^T; (*b*) C^T; (*c*) C^TC; (*d*) CC^T.

5.48 Ache (*a*) $A^2 = AA$; (*b*) $B^2 = BB$; (*c*) $C^2 = CC$.

Os problemas 5.49 a 5.52 se referem às seguintes matrizes:

$$A = \begin{bmatrix}1 & -1 & 2\\0 & 3 & 4\end{bmatrix}; \quad B = \begin{bmatrix}4 & 0 & -3\\-1 & -2 & 3\end{bmatrix}; \quad C = \begin{bmatrix}2 & -3 & 0 & 1\\5 & -1 & -4 & 2\\-1 & 0 & 0 & 3\end{bmatrix}; \quad D = \begin{bmatrix}2\\-1\\3\end{bmatrix}$$

5.49 Ache (*a*) $A + B$; (*b*) $A + C$; (*c*) $3A - 4B$.

5.50 Ache (*a*) AB; (*b*) AC; (*c*) AD.

5.51 Ache (*a*) BC; (*b*) BD; (*c*) CD.

5.52 Ache (*a*) A^T; (*b*) A^TB; (*c*) A^TC.

5.53 Seja $A = \begin{bmatrix}1 & 2\\3 & 6\end{bmatrix}$. Ache uma matriz 2×3 B com elementos distintos tal que $AB = 0$.

Matrizes Quadradas

5.54 Ache a diagonal de cada matriz:

(*a*) $\begin{bmatrix}2 & -7 & 8\\3 & -6 & -5\\4 & 0 & -1\end{bmatrix}$; (*b*) $\begin{bmatrix}1 & 2 & -9\\3 & 1 & 8\\5 & -6 & -1\end{bmatrix}$; (*c*) $\begin{bmatrix}3 & 4 & -8\\2 & -7 & 0\end{bmatrix}$.

5.55 Seja $A = \begin{bmatrix}2 & -5\\3 & 1\end{bmatrix}$. Ache:

(*a*) A^2 e A^3; (*b*) $f(A)$, onde $f(x) = x^3 - 2x^2 - 5$; (*c*) $g(A)$, onde $g(x) = x^2 - 3x + 17$.

5.56 Seja $B = \begin{bmatrix}4 & -2\\1 & -6\end{bmatrix}$. Ache:

(*a*) B^2 e B^3; (*b*) $f(B)$, onde $f(x) = x^2 + 2x - 22$; (*c*) $g(B)$, onde $g(x) = x^2 - 3x - 6$.

5.57 Seja $A = \begin{bmatrix}6 & -4\\3 & -2\end{bmatrix}$. Ache um vetor coluna não nulo $u = \begin{bmatrix}x\\y\end{bmatrix}$ tal que $Au = 4u$.

Determinantes e Inversas

5.58 Compute o determinante de cada matriz:

$$(a)\ \begin{bmatrix}2 & 5\\ 4 & 1\end{bmatrix};\quad (b)\ \begin{bmatrix}6 & 1\\ 3 & -2\end{bmatrix};\quad (c)\ \begin{bmatrix}4 & -5\\ 0 & 2\end{bmatrix};\quad (d)\ \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix};\quad (e)\ \begin{bmatrix}-2 & 8\\ -5 & -2\end{bmatrix}.$$

5.59 Compute o determinante de cada matriz:

$$(a)\ \begin{bmatrix}2 & 1 & 1\\ 0 & 5 & -2\\ 1 & -3 & 4\end{bmatrix};\quad (b)\ \begin{bmatrix}3 & -2 & -4\\ 2 & 5 & -1\\ 0 & 6 & 1\end{bmatrix};\quad (c)\ \begin{bmatrix}-2 & -1 & 4\\ 6 & -3 & -2\\ 4 & 1 & 2\end{bmatrix};\quad (d)\ \begin{bmatrix}7 & 6 & 5\\ 1 & 2 & 1\\ 3 & -2 & 1\end{bmatrix}.$$

5.60 Ache a inversa de cada matriz (se existir):

$$A=\begin{bmatrix}7 & 4\\ 5 & 3\end{bmatrix};\qquad B=\begin{bmatrix}2 & 3\\ 4 & 5\end{bmatrix};\qquad C=\begin{bmatrix}4 & -6\\ -2 & 3\end{bmatrix};\qquad =\begin{bmatrix}5 & -2\\ 6 & -3\end{bmatrix}$$

5.61 Ache a inversa de cada matriz (se existir):

$$A=\begin{bmatrix}1 & 2 & -4\\ -1 & -1 & 5\\ 2 & 7 & -3\end{bmatrix};\qquad B=\begin{bmatrix}1 & -1 & 1\\ 0 & 2 & -2\\ 1 & 3 & -1\end{bmatrix};\qquad C=\begin{bmatrix}1 & 2 & 3\\ 2 & 5 & -1\\ 5 & 12 & 1\end{bmatrix}$$

Matrizes Escalonadas, Redução por Linhas, Eliminação Gaussiana

5.62 Reduza A à forma escalonada e, depois, à forma canônica por linhas, onde:

$$(a)\ A=\begin{bmatrix}1 & 2 & -1 & 2 & 1\\ 2 & 4 & 1 & -2 & 3\\ 3 & 6 & 2 & -6 & 5\end{bmatrix};\qquad (b)\ A=\begin{bmatrix}2 & 3 & -2 & 5 & 1\\ 3 & -1 & 2 & 0 & 4\\ 4 & -5 & 6 & -5 & 7\end{bmatrix}.$$

5.63 Usando apenas 0s e 1s, liste todas as possíveis matrizes 2×2 na forma escalonada.

5.64 Usando apenas 0s e 1s, ache o número de possíveis matrizes 3×3 na forma canônica por linhas.

5.65 Resolva cada sistema usando sua matriz aumentada M.

$$(a)\ \begin{aligned}x+2y-4z&=-3\\ 2x+6y-5z&=2\\ 3x+11y-4z&=12\end{aligned}\qquad (b)\ \begin{aligned}x+2y-4z&=3\\ 2x+6y-5z&=10\\ 3x+10y-6z&=14\end{aligned}$$

5.66 Resolva cada sistema usando sua matriz aumentada M.

$$(a)\ \begin{aligned}x-3y+2z-t&=2\\ 3x-9y+7z-t&=7\\ 2x-6y+7z+4t&=7\end{aligned}\qquad (b)\ \begin{aligned}x+2y+3z&=7\\ x+3y+z&=6\\ 2x+6y+5z&=15\\ 3x+10y+7z&=23\end{aligned}$$

Problemas Variados

5.67 Seja $A=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$. Ache A^n.

5.68 Diz-se que duas matrizes A e B comutam se $AB=BA$. Ache todas as matrizes $\begin{bmatrix}x & y\\ z & t\end{bmatrix}$ que comutam com $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$.

5.69 Sejam $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ matrizes booleanas.

Ache as matrizes booleanas: (*a*) $A + B$; (*b*) AB; (*c*) BA; (*d*) A^2; (*e*) B^2.

Respostas dos Problemas Complementares

5.38 (*a*) $(-3, -16, 10)$; (*b*) $(-5, -16, 24)$; (*c*) $(22, 23, 33)$.

5.39 (*a*) $-3, -12, 8$; (*b*) $\sqrt{21}, \sqrt{35}, \sqrt{14}$.

5.40 (*a*) $(1, 1, 3, -15)$; (*b*) $(3, -14, 11, -32)$; (*c*) $(-2, -7, 2, 5)$; (*d*) $-6, -7, 6$; (*e*) $\sqrt{14}, \sqrt{12} = 2\sqrt{3}$, $\sqrt{18} = 3\sqrt{2}$.

5.41 (*a*) $(-1, 12, -35)^T$; (*b*) $(-8, 22, -24)^T$; (*c*) $-15, -27, 34$; (*d*) $\sqrt{26}, \sqrt{30}, 7$.

5.42 (*a*) $x = 2, y = -1$; (*b*) $x = 3, y = 2$.

5.43 $x = 3, y = -1, z = 2$.

5.44 (*a*) $\begin{bmatrix} -5 & 10 \\ 27 & -34 \end{bmatrix}$; (*b*) $\begin{bmatrix} 4 & 4 & 3 \\ 6 & -2 & 4 \end{bmatrix}$; (*c*) $= \begin{bmatrix} -7 & -27 & 11 \\ -8 & 36 & -37 \end{bmatrix}$.

5.45 $AB = \begin{bmatrix} -7 & 14 \\ 39 & -28 \end{bmatrix}$; $BA = \begin{bmatrix} 5 & 10 \\ 15 & -40 \end{bmatrix}$.

5.46 $AC = \begin{bmatrix} 5 & 9 & -6 \\ -5 & -33 & 32 \end{bmatrix}$; $AD = \begin{bmatrix} 11 & -9 & 17 \\ -7 & 53 & -39 \end{bmatrix}$; $BC = \begin{bmatrix} 5 & -15 & 20 \\ 8 & 60 & -59 \end{bmatrix}$; $BD = \begin{bmatrix} 15 & 35 & -5 \\ 10 & -98 & 69 \end{bmatrix}$.

5.47 $A^T = \begin{bmatrix} 1 & 3 \\ 2 & -4 \end{bmatrix}$; $C^T = \begin{bmatrix} 1 & 2 \\ -3 & 6 \\ 4 & -5 \end{bmatrix}$; $C^TC = \begin{bmatrix} 5 & 9 & -6 \\ 9 & 45 & -42 \\ -6 & -42 & 41 \end{bmatrix}$; $CC^T = \begin{bmatrix} 26 & -36 \\ -36 & 65 \end{bmatrix}$.

5.48 $A^2 = \begin{bmatrix} 7 & -6 \\ -9 & 22 \end{bmatrix}$; $B^2 = \begin{bmatrix} 25 & 0 \\ -72 & 49 \end{bmatrix}$; C^2 é não definido.

5.49 (*a*) $\begin{bmatrix} 5 & -1 & -1 \\ -1 & 1 & 7 \end{bmatrix}$; (*b*) não definido; (*c*) $\begin{bmatrix} -13 & -3 & 18 \\ 4 & 17 & 0 \end{bmatrix}$

5.50 AB é não definido; $AC = \begin{bmatrix} -5 & -22 & 4 & 5 \\ 11 & -3 & -12 & 18 \end{bmatrix}$; $AD = \begin{bmatrix} 9 \\ 9 \end{bmatrix}$.

5.51 $BC = \begin{bmatrix} 11 & -12 & 0 & -5 \\ -15 & 5 & 8 & 4 \end{bmatrix}$; $BD = \begin{bmatrix} 11 \\ 9 \end{bmatrix}$; CD é não definido.

5.52 $\bar{A} = \begin{bmatrix} 1 & 0 \\ -1 & 3 \\ 2 & 4 \end{bmatrix}$; $A^TB = \begin{bmatrix} 4 & 0 & -3 \\ -7 & -6 & 12 \\ 4 & -8 & 6 \end{bmatrix}$; A^Té não definido.

5.53 $B = \begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix}$.

5.54 (*a*) $[2, -6, -1]$; (*b*) $[1, 1, -1]$; (*c*) não definido.

5.55 $A^2 = \begin{bmatrix} -11 & -15 \\ 9 & -14 \end{bmatrix}$; $A^3 = \begin{bmatrix} -67 & 40 \\ -24 & -59 \end{bmatrix}$; $f(A) = \begin{bmatrix} -50 & 70 \\ -42 & -36 \end{bmatrix}$; $g(A) = 0$.

5.56 $B^2 = \begin{bmatrix} 14 & 4 \\ -2 & 34 \end{bmatrix}$; $B^3 = \begin{bmatrix} 60 & -52 \\ 26 & -200 \end{bmatrix}$; $f(B) = 0$; $g(B) = \begin{bmatrix} -4 & 10 \\ -5 & 46 \end{bmatrix}$.

5.57 $u = (2a, a)^T$, para todo a não nulo.

5.58 (*a*) -18; (*b*) -15; (*c*) 8; (*d*) 1; (*e*) 44.

5.59 (*a*) 21; (*b*) -11; (*c*) 100; (*d*) 0.

5.60 $A^{-1} = \begin{bmatrix} 3 & -4 \\ -5 & 7 \end{bmatrix}$; $B^{-1} = \begin{bmatrix} -\frac{5}{2} & \frac{3}{2} \\ 2 & -1 \end{bmatrix}$; C^{-1} é não definido; $D^{-1} = \begin{bmatrix} 1 & -\frac{2}{3} \\ 2 & -\frac{5}{3} \end{bmatrix}$.

5.61 $A^{-1} = \begin{bmatrix} -16 & -11 & 3 \\ \frac{7}{2} & \frac{5}{2} & -\frac{1}{2} \\ -\frac{5}{2} & -\frac{3}{2} & \frac{1}{2} \end{bmatrix}$; $B^{-1} = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & -1 & \frac{1}{2} \end{bmatrix}$; C^{-1} é não definido.

5.62 (*a*) $\begin{bmatrix} 1 & 2 & -1 & 2 & 1 \\ 0 & 0 & 3 & -6 & 1 \\ 0 & 0 & 0 & -6 & 1 \end{bmatrix}$ e $\begin{bmatrix} 1 & 2 & 0 & 0 & \frac{4}{3} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\frac{1}{6} \end{bmatrix}$.

(*b*) $\begin{bmatrix} 2 & 3 & -2 & 5 & 1 \\ 0 & -11 & 10 & -15 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ e $\begin{bmatrix} 1 & 0 & \frac{4}{11} & \frac{5}{11} & \frac{13}{11} \\ 0 & 1 & -\frac{10}{11} & \frac{15}{11} & -\frac{5}{11} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$.

5.63 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

5.64 Existem 13.

5.65 (*a*) $x = 3, y = 1, z = 2$; (*b*) sem solução.

5.66 (*a*) $x = 3y + 5t, y = 1 - 2t$; (*b*) $x = 2, y = 1, z = 1$.

5.67 $A^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}$.

5.68 $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$.

5.69 $A + B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$; $AB = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$; $BA = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$; $A^2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$; $B^2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$.

Capítulo 6

Contagem

6.1 INTRODUÇÃO: PRINCÍPIOS BÁSICOS DE CONTAGEM

A análise combinatória, que inclui o estudo de permutações, combinações e partições, trata da determinação do número de possibilidades lógicas de algum evento sem necessariamente identificar todos os casos. Existem dois princípios básicos de contagem usados no decorrer deste texto.

Princípio da regra da soma: Suponha que algum evento E pode ocorrer de m maneiras e que um segundo evento F pode ocorrer de n maneiras, e suponha que ambos os eventos não podem ocorrer simultaneamente. Então, E ou F podem ocorrer de $m + n$ maneiras. Mais genericamente, suponha que um evento E_1 pode ocorrer de n_1 maneiras, um segundo evento E_2 pode ocorrer de n_2 maneiras, e que um terceiro evento E_3 pode ocorrer de n_3 maneiras, ..., e suponha que dois eventos não podem ocorrer ao mesmo tempo. Então, algum dos eventos pode ocorrer de $n_1 + n_2 + n_3 + \ldots$, maneiras.

Exemplo 6.1

(*a*) Suponha que existe oito professores do sexo masculino e cinco professores do sexo feminino ministrando aulas de cálculo. Um estudante pode escolher um professor de cálculo de de $8 + 5 = 13$ maneiras.

(*b*) Suponha que E é o evento de escolher um número primo menor do que 10, e suponha que F é o evento de escolher um número par menor do que 10. Então, E pode ocorrer de quatro maneiras [2, 3, 5, 7], e F pode ocorrer de quatro maneiras [2, 4, 6,8]. Entretanto, E ou F não podem ocorrer de $4 + 4 = 8$ maneiras, uma vez que 2 é um primo menor do que 10 e um número par menor do que 10. De fato, E ou F podem ocorrer de apenas $4 + 4 - 1 = 7$ maneiras.

(*c*) Suponha que E é o evento de escolher um número primo entre 10 e 20, e suponha que F é o evento de escolher um número par entre 10 e 20. Então, E pode ocorrer de quatro maneiras [11, 13, 17, 19], e F pode ocorrer de quatro maneiras [12, 14, 16, 18]. Assim, E ou F podem ocorrer de $4 + 4 = 8$ maneiras, uma vez que agora nenhum dos números pares é primo.

Princípio da regra do produto: Suponha que existe um evento E que pode ocorrer de m maneiras e, independentemente deste evento, que existe um segundo evento F que pode ocorrer de n maneiras. As combinações de E e F ocorrem de mn maneiras. Mais genericamente, suponha que um evento E_1 pode ocorrer de n_1 maneiras, e, seguindo E_1, um segundo evento E_2 pode ocorrer de n_2 maneiras, e, seguindo E_2, um terceiro evento E_3 pode ocorrer de n_3 maneiras, e assim por diante. Então, todos os eventos podem ocorrer, na ordem indicada, de $n_1 \cdot n_2 \cdot n_3 \cdots$ maneiras.

Exemplo 6.2

(*a*) Suponha que uma placa de carro contém duas letras seguidas por três algarismos, sendo o primeiro dígito não nulo. Quantas placas de carro podem ser impressas?

Existem 26 possibilidades para cada letra, o primeiro algarismo tem nove possibilidades e cada um dos outros dois tem 10. Portanto,

$$26 \cdot 26 \cdot 9 \cdot 10 \cdot 10 = 608\,400$$

placas distintas podem ser impressas.

(*b*) De quantas maneiras uma organização com 26 membros pode eleger um presidente, um tesoureiro e um secretário (assumindo que ninguém pode ser eleito para mais de uma posição)?

O presidente pode ser eleito de 26 maneiras; a seguir, o tesoureiro pode ser eleito de 25 maneiras distintas (já que a pessoa escolhida como presidente não é elegível para tesoureiro); e, a seguir, o secretário pode ser eleito de 24 maneiras diferentes. Portanto, pelo princípio de contagem acima, existem

$$26 \cdot 25 \cdot 24 = 15\,600$$

maneiras distintas pelas quais a organização pode eleger os membros para os cargos.

Existe um conjunto de interpretações teóricas dos dois princípios de contagem acima. Especificamente, suponha que $n(A)$ denote o número de elementos em um conjunto A. Então:

(1) **Princípio da regra da soma:** se A e B são conjuntos disjuntos, então:

$$n(A \cup B) = n(A) + n(B)$$

(2) **Princípio da regra do produto:** seja $A \times B$ o produto cartesiano dos conjuntos A e B. Então:

$$n(A \times B) = n(A) \cdot n(B)$$

6.2 NOTAÇÃO FATORIAL

O produto dos inteiros positivos de 1 até n, inclusive, é denotado por $n!$ (lê-se "n fatorial"):

$$n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-2)(n-1)n$$

Em outras palavras, $n!$ é definido por:

$$1! = 1 \qquad \text{e} \qquad n! = n \cdot (n-1)!$$

Também é conveniente definir $0! = 1$.

Exemplo 6.3

(*a*) $2! = 1 \cdot 2 = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24,$

$5! = 5 \cdot 4! = 5 \cdot 24 = 120, \qquad 6! = 6 \cdot 5! = 6 \cdot 120 = 720.$

(*b*) $\dfrac{8!}{6!} = \dfrac{8 \cdot 7 \cdot 6!}{6!} = 8 \cdot 7 = 56, \qquad 12 \cdot 11 \cdot 10 = \dfrac{12 \cdot 11 \cdot 10 \cdot 9!}{9!} = \dfrac{12!}{9!},$

$\dfrac{12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3} = 12 \cdot 11 \cdot 10 \cdot \dfrac{1}{3!} = \dfrac{12!}{3!\,9!}.$

(*c*) $n(n-1)\cdots(n-r+1) = \dfrac{n(n-1)\cdots(n-r+1)(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1}{(n-r)(n-r-1)\cdots 3 \cdot 2 \cdot 1} = \dfrac{n!}{(n-r)!}.$

$\dfrac{n(n-1)\cdots(n-r+1)}{1 \cdot 2 \cdot 3 \cdots (r-1)r} = n(n-1)\cdots(n-r+1) \cdot \dfrac{1}{r!} = \dfrac{n!}{(n-r)!} \cdot \dfrac{1}{r!} = \dfrac{n!}{r!(n-r)!}.$

6.3 COEFICIENTES BINOMIAIS

O símbolo $\binom{n}{r}$ (lê-se "nCr"), onde r e n são inteiros positivos com $r \le n$, é definido como a seguir:

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1\cdot 2\cdot 3\cdots(r-1)r}$$

Pelo Exemplo 6.3(c), vemos que

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{1\cdot 2\cdot 3\cdots(r-1)r} = \frac{n!}{r!(n-r)!}$$

Porém, $n-(n-r)=r$; logo, temos a seguinte importante relação:

$$\binom{n}{n-r} = \binom{n}{r} \text{ ou, em outras palavras, se } a+b=n, \text{ então } \binom{n}{a} = \binom{n}{b}$$

Exemplo 6.4

(a) $\binom{8}{2} = \frac{8\cdot 7}{1\cdot 2} = 28$, $\binom{9}{4} = \frac{9\cdot 8\cdot 7\cdot 6}{1\cdot 2\cdot 3\cdot 4} = 126$, $\binom{12}{5} = \frac{12\cdot 11\cdot 10\cdot 9\cdot 8}{1\cdot 2\cdot 3\cdot 4\cdot 5} = 792$,
$\binom{10}{3} = \frac{10\cdot 9\cdot 8}{1\cdot 2\cdot 3} = 120$, $\binom{13}{1} = \frac{13}{1} = 13$.

Note que $\binom{n}{r}$ tem exatamente r fatores tanto no numerador quanto no denominador.

(b) Compute $\binom{10}{7}$. Por definição,

$$\binom{10}{7} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7} = 120$$

Por outro lado, $10-7=3$; e logo, também podemos computar $\binom{10}{7}$ como a seguir:

$$\binom{10}{7} = \binom{10}{3} = \frac{10\cdot 9\cdot 8}{1\cdot 2\cdot 3} = 120$$

Observe que o segundo método poupa espaço e tempo.

Coeficientes Binomiais e o Triângulo de Pascal

Os números $\binom{n}{r}$ são chamados os coeficientes binomiais, uma vez que aparecem como coeficientes na expansão de $(a+b)^n$. Especificamente, pode-se provar que:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Os coeficientes das potências sucessivas de $a+b$ podem ser organizados em um *array* triangular de números, chamado triângulo de Pascal, como na Figura 6-1. Os números do triângulo de Pascal têm as seguintes propriedades:

(i) O primeiro número e o último número em cada linha são 1.

(ii) Qualquer outro número no *array* pode ser obtido adicionando os dois números que aparecem diretamente acima dele. Por exemplo, $10 = 4+6$, $15 = 5+10$, $20 = 10+10$.

Como os números que aparecem no triângulo de Pascal são coeficientes binomiais, a propriedade (ii) do triângulo de Pascal vem do seguinte teorema (provado no Problema 6.7):

Teorema 6-1: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

$$(a+b)^0 = 1$$
$$(a+b)^1 = a + b$$
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$
$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$
$$(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$$
$$\cdots\cdots\cdots\cdots$$

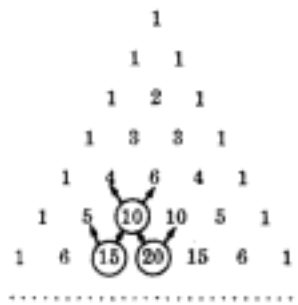


Fig. 6-1 Triângulo de Pascal

6.4 PERMUTAÇÕES

Qualquer arranjo de um conjunto de n objetos numa ordem dada é dito uma *permutação* dos objetos (usando todos a cada vez). Qualquer arranjo de $r \leq n$ desses objetos em uma ordem dada é dito uma *r-permutação* ou uma *permutação de n objetos* (tomando r a cada vez.). Considere, por exemplo, o conjunto de letras a, b, c e d. Então:

(i) *bdca*, *dcba* e *acdb* são permutações das quatro letras tomando todas a cada vez.

(ii) *bad*, *adb*, *cbd* e *bca* são permutações das quatro letras tomando três a cada vez.

(iii) *ad*, *cb*, *da* e *bd* são permutações das quatro letras tomadas duas a cada vez.

O número de permutações de n objetos, tomando r a cada vez, é denotado por

$$P(n, r),\ {}_nP_r,\ P_{n,r},\ P_r^n \text{ ou } (n)_r$$

Usaremos $P(n, r)$. Antes de deduzirmos a fórmula geral para $P(n, r)$, consideramos um caso particular.

Exemplo 6.5 Ache o número de permutações de seis objetos, A, B, C, D, E, F, tomando três a cada vez. Em outras palavras, ache o número de "palavras de três letras" usando apenas as seis letras dadas sem repetições.

Represente uma palavra genérica de três letras pelas três caixas seguintes:

A primeira letra pode ser escolhida de seis maneiras distintas; a seguir, a segunda letra pode ser escolhida de cinco maneiras distintas; e, a seguir, a terceira letra pode ser escolhida de quatro maneiras diferentes. Escreva cada número na caixa apropriada, como a seguir:

Portanto, pelo princípio fundamental de contagem, existem $6 \cdot 5 \cdot 4 = 120$ palavras possíveis de três letras, sem repetições, a partir das seis letras, ou existem 120 permutações de seis objetos tomando três de cada vez.

$$P(6, 3) = 120$$

Dedução da Fórmula de $P(n, r)$

A dedução da fórmula do número de permutações de n objetos tomando r de cada vez, ou o número de r-permutações de n objetos, $P(n, r)$, segue o procedimento adotado no exemplo anterior. O primeiro elemento de uma r-permutação de n objetos pode ser escolhido de n maneiras diferentes; a seguir, o segundo elemento da permutação pode ser escolhido de $n - 1$ maneiras diferentes; e, a seguir, o terceiro elemento da permutação pode ser escolhido de $n - 2$ maneiras. Continuando deste modo, temos o r-ésimo (último) elemento em uma r permutação que pode ser escolhido de $n - (r - 1) = n - r + 1$ maneiras. Então, pelo princípio fundamental de contagem, temos

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

Pelo Exemplo 6.3(c), vemos que

$$n(n-1)(n-2)\cdots(n-r+1) = \frac{n(n-1)(n-2)\cdots(n-r+1)\cdot(n-r)!}{(n-r)!} = \frac{n!}{(n-r)!}$$

Portanto, provamos o teorema seguinte.

Teorema 6-2: $P(n, r) = \dfrac{n!}{(n-r)!}$.

No caso especial em que $r = n$, temos

$$P(n, n) = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = n!$$

Conseqüentemente, temos o corolário seguinte.

Corolário 6-3: existem $n!$ permutações de n objetos (tomando todos a cada vez).

Por exemplo, existem $3! = 1 \cdot 2 \cdot 3 = 6$ permutações das três letras a, b e c. São elas, abc, acb, bac, bca e cab, cba.

Permutações com Repetições

Freqüentemente, desejamos saber o número de permutações de um *multiset*[†], isto é, um conjunto de objetos dos quais alguns são equivalentes. Vamos usar

$$P(n; n_1, n_2, \ldots, n_r)$$

para denotar o número de permutações de n objetos dos quais n_1 são equivalentes, n_2 são equivalentes, ..., n_r são equivalentes. A fórmula geral é:

Teorema 6-4: $P(n; n_1, n_2, \ldots, n_r) = \dfrac{n!}{n_1!n_2!\cdots n_r!}$.

Demonstramos o teorema acima com um exemplo particular. Suponha que queiramos formar todas as possíveis "palavras" de cinco letras usando as letras da palavra "BABBY". Existem $5! = 120$ permutações dos objetos B_1, A, B_2, B_3, Y, onde os três Bs são distintos. Observe que as seis permutações seguintes

$$B_1B_2B_3AY, \quad B_2B_1B_3AY, \quad B_3B_1B_2AY, \quad B_1B_3B_2AY, \quad B_2B_3B_1AY, \quad B_3B_2B_1AY,$$

produzem a mesma palavra quando os índices são removidos. O 6 vem do fato de que existem $3! = 3 \cdot 2 \cdot 1 = 6$ maneiras diferentes de posicionar os três Bs nas três primeiras posições da permutação. Isto é verdade para cada conjunto de três posições nas quais os Bs podem aparecer. Conseqüentemente, existem

$$P(5; 3) = \frac{5!}{3!} = \frac{120}{6} = 20$$

palavras de cinco letras que podem ser formadas usando as letras da palavra "BABBY".

[†] N. de T. Termo encontrado com freqüência nos textos de ciência da computação em português.

Exemplo 6.6

(*a*) Quantas palavras de sete letras podem ser formadas usando as letras da palavra "BENZENE"? Procuramos o número de permutações de três objetos dos quais três são equivalentes (os três Es) e dois são equivalentes (os dois Ns). Pelo Teorema 6.4, o número de tais palavras é:

$$P(7;3,2) = \frac{7!}{3!\,2!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 420$$

(*b*) Quantos sinais diferentes, cada um consistindo em oito bandeiras presas a uma linha vertical, podem ser formadas a partir de um conjunto de quatro bandeiras vermelhas indistinguíveis, três bandeiras brancas indistinguíveis, e uma bandeira azul? Procuramos o número de permutações de oito objetos dos quais quatro são equivalentes e três são equivalentes. O número de sinais é:

$$P(8;4,3) = \frac{8!}{4!\,3!} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 3 \cdot 2 \cdot 1} = 280$$

6.5 COMBINAÇÕES

Suponha que tenhamos um conjunto de n objetos. Uma *combinação* desses n objetos à taxa r é uma seleção de r objetos cuja ordem não importa. Em outras palavras, uma r-combinação de um conjunto de n objetos é qualquer subconjunto de r elementos. Por exemplo, as combinações das letras a, b, c e d à taxa três são:

$$\{a,b,c\}, \quad \{a,b,d\}, \quad \{a,c,d\}, \quad \{b,c,d\} \qquad \text{ou simplesmente} \qquad abc,\ abd,\ acd,\ bcd$$

Observe que as seguintes combinações são iguais:

$$abc,\ acb,\ bac,\ bca,\ cab \text{ e } cba$$

Isto é, cada uma delas denota o mesmo conjunto $\{a, b, c\}$.

O número de combinações de n objetos à taxa r é denotado por $C(n, r)$. Os símbolos ${}_nC_r$, $C_{n,r}$ e C_r^n também aparecem em vários textos. Antes de dar a fórmula geral para $C(n, r)$, consideramos um caso especial.

Exemplo 6.7 Ache o número de combinações de quatro objetos a, b, c e d à taxa 3.

Cada combinação consistindo em três objetos determina 3! = 6 permutações na combinação, como representado na Figura 6-2. Portanto, o número de combinações multiplicado por 3! é igual ao número de permutações; isto é,

$$C(4,3) \cdot 3! = P(4,3) \qquad \text{ou} \qquad C(4,3) = \frac{P(4,3)}{3!}$$

Mas $P(4,3) = 4 \cdot 3 \cdot 2 = 24$, e $3! = 6$; portanto, $C(4,3) = 4$, como se observa na Figura 6-2.

Combinação	Permutações
abc	***abc, acb, bac, bca, cab, cba***
abd	***abd, adb, bad, bda, dab, dba***
acd	***acd, adc, cad, cda, dac, dca***
bcd	***bcd, bdc, cbd, cdb, dbc, dcb***

Fig. 6-2

Fórmula para $C(n, r)$

Como qualquer combinação de n objetos à taxa r determina $r!$ permutações dos objetos na combinação, podemos concluir que

$$P(n,r) = r!C(n,r)$$

Portanto, obtemos

Teorema 6-5: $C(n,r) = \dfrac{P(n,r)}{r!} = \dfrac{n!}{r!(n-r)!}$

Lembre que o coeficiente binomial $\binom{n}{r}$ foi definido como $\dfrac{n!}{r!(n-r)!}$; logo, $C(n,r) = \binom{n}{r}$

Usaremos $C(n, r)$ e $\binom{n}{r}$ indistintamente.

Exemplo 6.8

(*a*) Quantos comitês de três podem ser formados com oito pessoas?

$$C(8,3) = \binom{8}{3} = \frac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3} = 56$$

(*b*) Um fazendeiro compra três vacas, dois porcos e quatro galinhas de um homem que tem seis vacas, cinco porcos e oito galinhas. Quantas escolhas tem o fazendeiro?

O fazendeiro pode escolher as vacas de $\binom{6}{3}$ maneiras, os porcos de $\binom{5}{2}$ maneiras e as galinhas de $\binom{8}{4}$ maneiras.

Portanto, juntando tudo, ele pode escolher os animais em

$$\binom{6}{3}\binom{5}{2}\binom{8}{4} = \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} \cdot \frac{5 \cdot 4}{1 \cdot 2} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3 \cdot 4} = 20 \cdot 10 \cdot 70 = 14.000 \text{ maneiras.}$$

6.6 O PRINCÍPIO DA CASA DO POMBO

Muitos resultados, na teoria combinatória, vêm da seguinte afirmação quase óbvia.

Princípio da casa de pombo:[†] Se n casas de pombos são ocupadas por $n + 1$ ou mais pombos, então pelo menos uma casa é ocupada por mais de um pombo.

Esse princípio pode ser aplicado a muitos problemas para os quais queremos mostrar que uma determinada situação ocorre.

Exemplo 6.9

(*a*) Suponha que um departamento tem 13 professores (pombos). Então, dois dos professores (pombos) nasceram no mesmo mês (casa de pombos).

(*b*) Suponha que um saco de lavanderia contém muitas meias vermelhas, brancas e azuis. Então, é necessário pegar apenas quatro meias (pombos) para ter certeza de obter um par com uma única cor (casa de pombo).

(*c*) Ache o menor número de elementos que devem ser escolhidos em um conjunto $S = \{1, 2, 3, \ldots, 9\}$ para se ter certeza de que dois dos números somem 10.

Aqui as casas de pombos são os cinco conjuntos {1,9}, {2,8}, {3,7}, {4,6} e {5}. Portanto, qualquer escolha de seis elementos (pombos) de S garantirá que dois dos números somem dez.

O princípio da casa de pombos é generalizado como a seguir.

Princípio da casa de pombos generalizado: Se n casas de pombo são ocupadas por $kn + 1$ ou mais pombos, onde k é um inteiro positivo, então pelo menos uma casa de pombo é ocupada por $k + 1$ ou mais pombos.

Exemplo 6.10

(*a*) Ache o número mínimo de estudantes de uma turma que garante que pelo menos três deles nasceram no mesmo mês.

Aqui $n = 12$ meses é o número de casas de pombo, e $k + 1 = 3$, ou $k = 2$. Portanto, dentre $kn + 1 = 25$ estudantes (pombos), três nasceram no mesmo mês.

(*b*) Suponha que um saco de lavanderia contém muitas meias vermelhas, brancas e azuis. Ache o número de meias que é preciso escolher a fim de obter dois pares (quatro meias) da mesma cor.

Aqui existem $n = 3$ cores (casas de pombos), e $k + 1 = 4$, ou $k = 3$. Assim, dentre quaisquer $kn + 1 = 10$ meias (pombos), quatro têm a mesma cor.

[†] N. de T. No original, *pigeonhole principle*; escolhemos a tradução mais freqüente em ciência da computação, embora seja comum em outras áreas a denominação "princípio do escaninho".

6.7 O PRINCÍPIO DE INCLUSÃO-EXCLUSÃO

Sejam A e B quaisquer conjuntos finitos. Então,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Em outras palavras, para achar o número n $(A \cup B)$ de elementos na união $A \cup B$, somamos $n(A)$ e $n(B)$ e então subtraímos $n(A \cap B)$; isto é, "incluímos" $n(A)$ e $n(B)$ e então "excluímos" $n(A \cap B)$. Isto segue do fato de que, quando somamos $n(A)$ e $n(B)$, contamos os elementos da interseção duas vezes. Este princípio vale para qualquer número de conjuntos. Enunciamos o princípio, primeiramente, para três conjuntos.

Teorema 6-6: para quaisquer conjuntos finitos A, B e C, temos

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$

Isto é, "incluímos" $n(A)$, $n(B)$ e $n(C)$, excluímos $n(A \cap B)$, $n(A \cap C)$, $n(B \cap C)$ e incluímos $n(A \cap B \cap C)$.

Exemplo 6.11 Ache o número de estudantes de matemática que estudam pelo menos uma das línguas, francês, alemão e russo, sabendo os dados seguintes:

65 estudam francês	20 estudam francês e alemão
45 estudam alemão	25 estudam francês e russo
42 estudam russo	15 estudam alemão e russo
	8 estudam as três línguas

Queremos achar $n(F \cup A \cup R)$, onde F, A e R denotam os conjuntos de alunos estudando francês, alemão e russo, respectivamente.

Pelo princípio de inclusão-exclusão,

$$n(F \cup A \cup R) = n(F) + n(A) + n(R) - n(F \cap A) - n(F \cap R) - n(A \cap R) + n(F \cap A \cap R)$$

$$= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100$$

Assim, 100 estudantes estudam pelo menos uma das línguas.

Agora, suponha que temos um número finito qualquer de conjuntos finitos, $A_1, A_2, \ldots, A_m$. Seja s_k a soma das cardinalidades

$$n(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k})$$

de todas as possíveis k-uplas de interseções dos m conjuntos dados. Então, temos o seguinte princípio geral de inclusão-exclusão.

Teorema 6-7: $n(A_1 \cup A_2 \cup \cdots \cup A_m) = s_1 - s_2 + s_3 - \cdots + (-1)^{m-1} s_m$.

6.8 PARTIÇÕES ORDENADAS E NÃO ORDENADAS

Suponha que um saco contém sete bolas de gude numeradas de 1 a 7. Calculamos o número de maneiras que podemos retirar, primeiramente, duas bolas do saco, depois três bolas, e finalmente duas bolas. Em outras palavras, queremos calcular o número de *partições ordenadas*

$$[A_1, A_2, A_3]$$

do conjunto de sete bolas de gude em células A_1 contendo duas bolas, A_2 contendo três bolas e A_3 contendo duas bolas. Denominamos essas partições como ordenadas porque distinguimos

$$[\{1,2\}, \{3,4,5\}, \{6,7\}] \quad \text{e} \quad [\{6,7\}, \{3,4,5\}, \{1,2\}]$$

que definem a mesma partição de A.

Começamos com sete bolas no saco; logo, existem $\binom{7}{2}$ maneiras de retirar as primeiras duas bolas, i. e., de determinar a primeira célula A_1. Depois disto, existem cinco bolas no saco e $\binom{5}{3}$ maneiras de pegar as três bolas, i.é, de determinar a segunda célula A_2. Finalmente, restam duas bolas de gude no saco e, logo, existem $\binom{2}{2}$ maneiras de determinar a última célula A_3.

Portanto, existem

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7 \cdot 6}{1 \cdot 2} \cdot \frac{5 \cdot 4 \cdot 3}{1 \cdot 2 \cdot 3} \cdot \frac{2 \cdot 1}{1 \cdot 2} = 210$$

partições ordenadas distintas de A em células A_1 contendo duas bolas de gude, A_2 contendo três bolas de gude, e A_3 contendo duas bolas de gude.

Agora observe que

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!\,5!} \cdot \frac{5!}{3!\,2!} \cdot \frac{2!}{2!\,0!} = \frac{7!}{2!\,3!\,2!}$$

já que cada numerador, após o primeiro, é cancelado pelo segundo termo no denominador do fator prévio.

Pode-se mostrar que a discussão acima vale em geral. Para tanto, enunciamos

Teorema 6-8: suponha que A contém n elementos, e sejam $n_1, n_2, \ldots, n_r$ inteiros positivos cuja soma é n, isto é, $n_1 + n_2 + \cdots + n_r = n$. Então, existem

$$\frac{n!}{n_1!\,n_2!\,n_3! \cdots n_r!}$$

partições distintas ordenadas de A da forma $[A_1, A_2, \ldots, A_r]$, onde A_1 contém n_1 elementos, A_2 contém n_2 elementos, ..., e A_r contém n_r elementos.

Aplicamos esse teorema no próximo exemplo.

Exemplo 6.12 Ache o número m de maneiras que nove brinquedos podem ser divididos entre quatro crianças se a mais jovem deve receber três brinquedos e cada uma das outras, dois brinquedos.

Queremos achar o número m de partições ordenadas de nove brinquedos em quatro células contendo 3, 2, 2, 2 brinquedos, respectivamente. Pelo Teorema 6.8,

$$m = \frac{9!}{3!\,2!\,2!\,2!} = 7.560$$

Partições Não Ordenadas

Freqüentemente, desejamos particionar um conjunto A em uma coleção de subconjuntos $A_1, A_2, \ldots, A_r$ onde os subconjuntos, agora, não estão ordenados. Da mesma forma que o número de permutações com repetição foi obtido do número de permutações, dividindo por $k!$ quando k objetos eram equivalentes, também podemos obter o número de partições não ordenadas a partir do número de partições ordenadas, dividindo por $k!$ quando k dos conjuntos têm o mesmo número de elementos. Isso é ilustrado no próximo exemplo, no qual resolvemos o problema de duas maneiras.

Exemplo 6.13 Ache o número m de maneiras que 12 estudantes podem ser divididos em três times A_1, A_2 e A_3, de tal forma que cada time contenha quatro estudantes.

Método 1: Seja A um dos estudantes. Então, existem $\binom{11}{3}$ maneiras de escolher três outros estudantes para serem do mesmo time que A. Agora, seja B um estudante que não está no mesmo time que A; então, existem $\binom{7}{3}$ maneiras de escolher três estudantes entre os remanescentes para ficarem no mesmo time de B. Os quatro estudantes restantes constituem o terceiro time. Juntando todas as informações, o número de maneiras de dividir os estudantes é

$$m = \binom{11}{3} \cdot \binom{7}{3} = 165 \cdot 35 = 5775$$

Método 2: Observe que cada partição $\{A_1, A_2 \text{ e } A_3\}$ de estudantes pode ser organizada de $3! = 6$ maneiras como em uma partição ordenada. Pelo Teorema 6.8, existem $\dfrac{12!}{4!\,4!\,4!} = 34\,650$ partições ordenadas. Portanto, existem $m = 34\,650/6 = 5775$ partições (não ordenadas).

Problemas Resolvidos

Notação Fatorial e Coeficientes Binominais

6.1 Compute 4!, 5!, 6! e 7!.

$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$, $\quad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6 \cdot (5!) = 6 \cdot (120) = 720$,

$5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5 \cdot (4!) = 5 \cdot (24) = 120$, $\quad 7! = 7 \cdot (6!) = 7 \cdot (720) = 5040$.

6.2 Compute : (*a*) $\dfrac{13!}{11!}$; (*b*) $\dfrac{7!}{10!}$.

(*a*) $\dfrac{13!}{11!} = \dfrac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13 \cdot 12 = 156.$

Alternativamente, isto pode ser resolvido como a seguir:

$$\frac{13!}{11!} = \frac{13 \cdot 12 \cdot 11!}{11!} = 13 \cdot 12 = 156.$$

(*b*) $\dfrac{7!}{10!} = \dfrac{7!}{10 \cdot 9 \cdot 8 \cdot 7!} = \dfrac{1}{10 \cdot 9 \cdot 8} = \dfrac{1}{720}.$

6.3 Simplifique: (*a*) $\dfrac{n!}{(n-1)!}$; (*b*) $\dfrac{(n+2)!}{n!}$.

(*a*) $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = n$; alternativamente, $\dfrac{n!}{(n-1)!} = \dfrac{n(n-1)!}{(n-1)!} = n.$

(*b*) $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1}{(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1} = (n+2)(n+1) = n^2 + 3n + 2;$

Alternativamente, $\dfrac{(n+2)!}{n!} = \dfrac{(n+2)(n+1)n!}{n!} = (n+2)(n+1) = n^2 + 3n + 2.$

6.4 Compute: (*a*) $\binom{16}{3}$; (*b*) $\binom{12}{4}$.

Lembre que existem tantos fatores no numerador quanto no denominador.

(*a*) $\binom{16}{3} = \frac{16 \cdot 15 \cdot 14}{1 \cdot 2 \cdot 3} = 560$; (*b*) $\binom{12}{4} = \frac{12 \cdot 11 \cdot 10 \cdot 9}{1 \cdot 2 \cdot 3 \cdot 4} = 495$.

6.5 Compute: (*a*) $\binom{8}{5}$; (*b*) $\binom{9}{7}$.

(*a*) $\binom{8}{5} = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 56$ ou, como $8 - 5 = 3$, $\binom{8}{5} = \binom{8}{3} = \frac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3} = 56$.

(*b*) Como $9 - 7 = 2$, temos $\binom{9}{7} = \binom{9}{2} = \frac{9 \cdot 8}{1 \cdot 2} = 36$.

6.6 Prove: $\binom{17}{6} = \binom{16}{5} + \binom{16}{6}$.

Agora, $\binom{16}{5} + \binom{16}{6} = \frac{16!}{5!\,11!} + \frac{16!}{6!\,10!}$. Multiplique a primeira fração por $\frac{6}{6}$ e a segunda por $\frac{11}{11}$ para obter o mesmo denominador em ambas as frações; após, some:

$$\begin{aligned}\binom{16}{5} + \binom{16}{6} &= \frac{6 \cdot 16!}{6 \cdot 5! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11 \cdot 10!} = \frac{6 \cdot 16!}{6! \cdot 11!} + \frac{11 \cdot 16!}{6! \cdot 11!} \\ &= \frac{6 \cdot 16! + 11 \cdot 16!}{6! \cdot 11!} = \frac{(6 + 11) \cdot 16!}{6! \cdot 11!} = \frac{17 \cdot 16!}{6! \cdot 11!} = \frac{17!}{6! \cdot 11!} = \binom{17}{6}\end{aligned}$$

6.7 Prove o Teorema 6.1: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$.

(A técnica nesta demonstração é similar à do problema precedente.)

Agora, $\binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)! \cdot (n-r+1)!} + \frac{n!}{r! \cdot (n-r)!}$. Para obter o mesmo denominador em ambas as frações, multiplique a primeira fração por $\frac{r}{r}$ e a segunda fração por $\frac{n-r+1}{n-r+1}$. Portanto,

$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{r \cdot n!}{r \cdot (r-1)! \cdot (n-r+1)!} + \frac{(n-r+1) \cdot n!}{r! \cdot (n-r+1) \cdot (n-r)!} \\ &= \frac{r \cdot n!}{r!(n-r+1)!} + \frac{(n-r+1) \cdot n!}{r!(n-r+1)!} \\ &= \frac{r \cdot n! + (n-r+1) \cdot n!}{r!(n-r+1)!} = \frac{[r + (n-r+1)] \cdot n!}{r!(n-r+1)!} \\ &= \frac{(n+1)n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r}\end{aligned}$$

Permutações

6.8 Existem quatro linhas de ônibus entre A e B e três linhas entre B e C. De quantas maneiras um homem pode viajar (*a*) de ônibus de A para C passando por B? (*b*) com um percurso circular (ida e volta) de A para C passando por B? (*c*) com um percurso circular (ida e volta) de A para C passando por B, se ele não quiser usar uma linha de ônibus mais de uma vez?

(*a*) Existem quatro maneiras de ir de A para B e três maneiras de ir de B para C; logo, existem $4 \cdot 3 = 12$ maneiras de ir de A para C passando por B.

(*b*) Existem 12 maneiras de ir de A para C pelo caminho de B e 12 maneiras de retornar. Portanto, existem $12 \cdot 12 = 144$ maneiras de fazer o caminho circular.

(*c*) O homem viajará de A para B para C para B para A. Escreva essas letras conectando-as com setas como a seguir:

$$A \longrightarrow B \longrightarrow C \longrightarrow B \longrightarrow A$$

O homem pode viajar de quatro maneiras de A para B e de três maneiras de B para C, mas só pode viajar de duas maneiras de C para B e de três maneiras de B para A, já que não quer usar a mesma linha mais de uma vez. Coloque esses números sobre as setas correspondentes como a seguir:

$$A \xrightarrow{4} B \xrightarrow{3} C \xrightarrow{2} B \xrightarrow{3} A$$

Então, existem $4 \cdot 3 \cdot 2 \cdot 3 = 72$ maneiras de viajar por um caminho circular sem usar a mesma linha de ônibus mais de uma vez.

6.9 Suponha que não sejam permitidas repetições. (*a*) Quantos números de três dígitos podem ser formados usando os seis dígitos 2, 3, 5, 6, 7 e 9? (*b*) Quantos desses números são menores do que 400? (*c*) Quantos são pares?

Em cada caso, desenhe três caixas ☐ ☐ ☐ para representar um número arbitrário, e então escreva em cada caixa o número de dígitos que podem ser colocados ali.

(*a*) A caixa da esquerda pode ser preenchida de seis maneiras; posteriormente, a caixa do meio pode ser preenchida de cinco maneiras; e, finalmente, a caixa da direita pode ser preenchida de quatro maneiras: 6 5 4. Portanto, existem $6 \cdot 5 \cdot 4 = 120$ números.

(*b*) A caixa da esquerda pode ser preenchida de duas maneiras apenas; depois disto, a caixa do meio pode ser preenchida de cinco maneiras; e, finalmente, a caixa da direita pode ser preenchida de quatro maneiras: 2 5 4. Portanto, existem $2 \cdot 5 \cdot 4 = 40$ números.

(*c*) A caixa da direita pode ser preenchida de duas maneiras apenas (por 2 ou 6), já que os números devem ser pares; a caixa da esquerda pode ser preenchida de cinco maneiras; e, finalmente, a caixa do meio pode ser preenchida de quatro maneiras: 5 4 2. Portanto, existem $5 \cdot 4 \cdot 2 = 40$ números.

6.10 Ache o número de maneiras que sete pessoas podem se posicionar em uma festa: (*a*) em uma linha de sete cadeiras; (*b*) em torno de uma mesa circular.

(*a*) As sete pessoas podem se organizar em linha de $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 7!$ maneiras.

(*b*) Uma pessoa pode sentar-se em qualquer lugar da mesa. As outras seis podem se organizar de $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6!$ maneiras em torno da mesa.

(*c*) Isso é um exemplo de *permutação circular*. Em geral, n objetos podem ser organizados em círculo de $(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1 = (n-1)!$ maneiras.

6.11 Ache o número de permutações distintas que podem ser formadas com todas as letras de cada palavra: (*a*) **RADAR**; (*b*) **SUCESSO**.

(*a*) $\dfrac{5!}{2!\,2!} = 30$, já que existem cinco letras das quais duas são R e duas são A.

(*b*) $\dfrac{7!}{3!} = 840$, já que existem sete letras das quais três são S.

6.12 De quantas maneiras quatro livros de matemática, três de história, três de química e dois de sociologia podem ser organizados em uma prateleira de tal forma que todos os livros do mesmo assunto fiquem juntos?

Primeiramente os livros precisam ser organizados na prateleira em quatro unidades, de acordo com o assunto: ☐ ☐ ☐ ☐. A caixa do lado esquerdo pode ser preenchida por qualquer um dos quatro assuntos; a seguinte, por qualquer um dos três remanescentes; a próxima, por qualquer um dos dois remanescentes; e a caixa da direita, pelo último assunto: 4 3 2 1. Portanto, existem $4 \cdot 3 \cdot 2 \cdot 1 = 4!$ maneiras de organizar os livros na estante de acordo com o assunto.

Agora, em cada um dos casos acima, os livros de matemática podem ser arrumados de 4! maneiras; os livros de história, de 3! maneiras; os de química, de 3! maneiras; e os de sociologia, de 2! maneiras. Portanto, juntando todas as informações, existem $4! \cdot 4! \cdot 3! \cdot 3! \cdot 2! = 41\,472$ arranjos.

6.13 Ache n se: (*a*) $P(n,2) = 72$; (*b*) $P(n,4) = 42P(n,2)$; (*c*) $2P(n,2) + 50 = P(2n,2)$.

(*a*) $P(n,2) = n(n-1) = n^2 - n$; logo, $n^2 - n = 72$ or $n^2 - n - 72 = 0$ ou $(n-9)(n+8) = 0$. Como n deve ser positivo, a única resposta é $n = 9$.

(*b*) $P(n,4) = n(n-1)(n-2)(n-3)$ e $P(n,2) = n(n-1)$. Portanto,

$$n(n-1)(n-2)(n-3) = 42n(n-1) \quad \text{ou, se } n \neq 0, n \neq 1, \quad (n-2)(n-3) = 42$$
$$\text{ou} \quad n^2 - 5n + 6 = 42 \quad \text{ou} \quad n^2 - 5n - 36 = 0 \quad \text{ou} \quad (n-9)(n+4) = 0$$

Como n deve ser positivo, a única resposta é $n = 9$.

(*c*) $P(n,2) = n(n-1) = n^2 - n$ e $P(2n,2) = 2n(2n-1) = 4n^2 - 2n$. Logo,

$$2(n^2 - n) + 50 = 4n^2 - 2n \quad \text{ou} \quad 2n^2 - 2n + 50 = 4n^2 - 2n \quad \text{ou} \quad 50 = 2n^2 \quad \text{ou} \quad n^2 = 25$$

Como n deve ser positivo, a única resposta é $n = 5$.

Combinações

6.14 De quantas maneiras um comitê, constituído por três homens e duas mulheres, pode ser escolhido entre sete homens e cinco mulheres?

Os três homens podem ser escolhidos de $\binom{7}{3}$ maneiras, e as duas mulheres podem ser escolhidas de $\binom{5}{2}$ maneiras. Portanto, o comitê pode ser escolhido de

$$\binom{7}{3}\binom{5}{2} = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} \cdot \frac{5 \cdot 4}{1 \cdot 2} = 350 \text{ maneiras.}$$

6.15 Um saco contém seis bolas de gude brancas e quatro bolas de gude vermelhas. Ache o número de maneiras que quatro bolas podem ser retiradas do saco se (*a*) elas podem ser de qualquer cor; (*b*) duas devem ser brancas e duas vermelhas; (*c*) todas devem ter a mesma cor.

(*a*) As quatro bolas de gude (de qualquer cor) podem ser escolhidas entre onze bolas de $\binom{11}{4} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3 \cdot 4} = 330$ maneiras.

(*b*) As duas bolas brancas podem ser escolhidas de $\binom{6}{2}$ maneiras, e as duas vermelhas podem ser escolhidas de $\binom{5}{2}$ maneiras. Portanto, existem $\binom{6}{2}\binom{5}{2} = \frac{6 \cdot 5}{1 \cdot 2} \cdot \frac{5 \cdot 4}{1 \cdot 2} = 150$ maneiras de retirar duas bolas de gude brancas e duas bolas de gude vermelhas.

(*c*) Existem $\binom{6}{4} = 15$ maneiras de retirar quatro bolas de gude brancas, e $\binom{5}{4} = 5$ maneiras de retirar quatro bolas vermelhas. Assim, existem $15 + 5 = 20$ maneiras de retirar quatro bolas da mesma cor.

6.16 Quantos comitês de cinco pessoas com um determinado chefe podem ser selecionados entre doze pessoas?

O chefe pode ser escolhido de 12 maneiras e, depois, os outros quatro do comitê podem ser escolhidos entre os onze remanescentes de $\binom{11}{4}$ maneiras. Logo, existem $12 \cdot \binom{11}{4} = 12 \cdot 330 = 3960$ destes comitês.

Partições Ordenadas e Não Ordenadas

6.17 De quantas maneiras nove estudantes podem ser divididos em três times contendo quatro, três e dois estudantes, respectivamente?

Como todas as células contêm números diferentes de estudantes, o número de partições não ordenadas é igual ao número de partições ordenadas, $\frac{9!}{4!\,3!\,2!} = 1260$.

6.18 Existem 12 estudantes em uma classe. De quantas maneiras podem os 12 estudantes fazer quatro testes diferentes se cada três estudantes devem fazer o mesmo teste?

Método 1: Procuramos o número de partições ordenadas de 12 estudantes em células contendo três estudantes cada. Pelo Teorema 6.8, existem $\frac{12!}{3!\,3!\,3!\,3!} = 369\,600$ dessas partições.

Método 2: Existem $\binom{12}{3}$ maneiras de escolher três estudantes para fazer o primeiro teste; depois, existem $\binom{9}{3}$ maneiras de escolher três estudantes para fazer o segundo teste; e $\binom{6}{3}$ maneiras de escolher três estudantes para fazer o terceiro teste. Os estudantes remanescentes fazem o quarto teste. Juntando todas as informações, existem $\binom{12}{3}\binom{9}{3}\binom{6}{3} = (220)(84)(20) = 369.600$ maneiras para os estudantes fazerem os testes.

6.19 De quantas maneiras 12 estudantes podem ser divididos em quatro times, A_1, A_2, A_3 e A_4, de tal modo que cada time contenha três estudantes?

Método 1: Observe que cada partição $\{A_1, A_2, A_3, A_4\}$ de estudantes pode ser organizada de $4! = 24$ maneiras como em uma partição ordenada. Como (veja o problema anterior) existem $\frac{12!}{3!\,3!\,3!\,3!} = 369\,600$ dessas partições ordenadas, existem $369\,600/24 = 15\,400$ partições (não ordenadas).

Método 2: Seja A um dos estudantes. Existem $\binom{11}{2}$ maneiras de escolher dois outros estudantes para ficarem no mesmo time que A. Agora, seja B um estudante que não está no mesmo time que A. Então, existem $\binom{8}{2}$ maneiras de escolher dois estudantes, entre os remanescentes, para ficar no mesmo time que B. Agora, seja C um estudante que não está no time de A ou B. Então, existem $\binom{5}{2}$ maneiras de escolher dois estudantes para ficarem no mesmo time de C. Os três estudantes restantes constituem o quarto time. Portanto, juntando todas as informações, existem $\binom{11}{2}\binom{8}{2}\binom{5}{2} = (55)(28)(10) = 15\,400$ maneiras de dividir os estudantes.

O Princípio da Casa do Pombo

6.20 Suponha que existem n pares distintos de sapatos em um armário. Mostre que, se você escolher aleatoriamente $n + 1$ sapatos avulsos no armário, com certeza haverá entre eles um par.

Os n pares distintos constituem n pombos. Os $n + 1$ sapatos avulsos correspondem a $n + 1$ pombos. Portanto, haverá pelo menos uma casa de pombos com dois sapatos e, logo, certamente haverá pelo menos um par de sapatos.

6.21 Suponha que existem três homens e cinco mulheres em uma festa. Mostre que, se estas pessoas estiverem alinhadas em fila, pelo menos duas mulheres ocuparão posições consecutivas.

Considere o caso em que os homens estão posicionados de modo que dois homens não podem nem ocupar posições consecutivas nem estar em qualquer extremo da fila. Neste caso, os três homens geram quatro posições potenciais (casas

de pombos) para uma mulher se posicionar (em algum extremo da fila ou entre dois homens). Como existem cinco mulheres (pombos), pelo menos uma posição conterá duas mulheres que ocuparão, portanto, posições consecutivas. Se os homens estiverem posicionados em lugares adjacentes ou no final da fila, existe um número ainda menor de casas de pombos e, mais uma vez, duas mulheres terão posições consecutivas.

6.22 Ache o número mínimo de estudantes necessários que garanta que cinco deles pertencem à mesma turma (primeira série, segunda série, terceira série, quarta série).[7]

Aqui, as $n = 4$ turmas são as casas de pombos e $k + 1 = 5$; logo, $k = 4$. Portanto, entre quaisquer $kn + 1 = 17$ estudantes (pombos), cinco deles pertencem à mesma turma.

6.23 Um estudante precisa assistir a cinco aulas de três áreas do conhecimento. Muitas aulas são oferecidas para cada disciplina, mas o estudante não pode assistir a mais de duas turmas em qualquer uma das áreas.

(*a*) Usando o princípio da casa do pombo, mostre que o estudante assistirá a pelo menos duas aulas em alguma área.

(*b*) Usando o princípio de inclusão-exclusão, mostre que o estudante precisará assistir a pelo menos uma aula de cada área.

(*a*) As três áreas são as casas de pombos, e o estudante precisa assistir a cinco aulas (pombos). Portanto, o estudante precisa assistir a pelo menos duas aulas em alguma área.

(*b*) Sejam A, B e C três conjuntos disjuntos representando cada uma das áreas de conhecimento. Como os conjuntos são disjuntos, $n(A \cup B \cup C) = 5 = n(A) + n(B) + n(C)$. Como os estudantes podem assistir a, no máximo, duas aulas em qualquer área, a soma das aulas em quaisquer dois conjuntos, digamos A e B, precisa ser menor ou igual a 4. Portanto, $5 - [n(A) + n(B)] = n(C) \geq 1$. Logo, o estudante precisa assistir a pelo menos uma aula em cada área.

6.24 Seja L uma lista (não necessariamente em ordem alfabética) de 26 letras do alfabeto (que consiste em cinco vogais A, E, I, O, U e 21 consoantes). (*a*) Mostre que L tem uma sublista consistindo em quatro ou mais consoantes consecutivas. (*b*) Assumindo que L começa com uma vogal, por exemplo A, mostre que L tem uma sublista consistindo em cinco ou mais consoantes consecutivas.

(*a*) As cinco letras dividem L em seis sublistas (casas de pombos) de consoantes consecutivas. Aqui, $k + 1 = 4$ e, portanto, $k = 3$. Logo, $nk + 1 = 6(3) + 1 = 19 < 21$. Segue que pelo menos uma sublista tem no mínimo quatro consoantes consecutivas.

(*b*) Como L começa com uma vogal, as vogais remanescentes dividem L em $n = 5$ sublistas. Aqui $k + 1 = 5$ e, portanto, $k = 4$. Logo, $kn + 1 = 21$. Assim, alguma sublista tem pelo menos cinco consoantes consecutivas.

6.25 Ache o número mínimo n de inteiros a serem selecionados de $S = \{1, 2, \ldots, 9\}$ tal que: (*a*) a soma de dois dos n inteiros seja par; (*b*) a diferença de dois dos n inteiros seja 5.

(*a*) A soma de dois inteiros pares ou de dois inteiros ímpares é par. Considere os subconjuntos $\{1, 3, 5, 7, 9\}$ e $\{2, 4, 6, 8\}$ de S como casas de pombo. Logo, $n = 3$.

(*b*) Considere os cinco subconjuntos $\{1, 6\}$, $\{2, 7\}$, $\{3, 8\}$, $\{4, 9\}$, $\{5\}$ de S como casas de pombos. Então, $n = 6$ vai garantir que dois inteiros pertencerão a algum dos subconjuntos e que sua diferença será 5.

O Princípio de Inclusão-Exclusão

6.26 Existem 22 estudantes do sexo feminino e 18 estudantes do sexo masculino em uma sala de aula. Quantos estudantes existem no total?

Os conjuntos de estudantes do sexo masculino e feminino são disjuntos; portanto, o total é $t = 22 + 18 = 40$ estudantes.

6.27 Dentre 32 pessoas que guardam papel ou garrafas (ou ambos) para reciclar, 30 guardam papel e 14 guardam garrafas. Ache o número m de pessoas que (*a*) guardam ambos, (*b*) guardam apenas papel e (*c*) guardam apenas garrafas.

Sejam P e G os conjuntos de pessoas que guardam papel e garrafas, respectivamente. Pelo Teorema 6.7:

[7] N. de T. No original, *Freshman, Sophomore, Junior, Senior*.

(*a*) $m = n(P \cap G) = n(P) + n(G) - n(P \cup G) = 30 + 14 - 32 = 12.$

(*b*) $m = n(P \setminus G) = n(P) - n(P \cap G) = 30 - 12 = 18.$

(*c*) $m = n(G \setminus P) = n(G) - n(P \cap G) = 14 - 12 = 2.$

6.28 Sejam A, B, C e D cursos de, respectivamente, arte, biologia, química e teatro. Ache o número N de estudantes em um dormitório, considerando os seguintes dados:

12 cursam A,	5 cursam A e B,	3 cursam A, B, Q,
20 cursam B,	7 cursam A e Q,	2 cursam A, B, T,
20 cursam Q,	4 cursam A e T,	2 cursam B, Q, T,
8 cursam T,	16 cursam B e Q,	3 cursam A, Q, T,
	4 cursam B e T,	2 cursam os quatro.
	3 cursam Q e T,	71 não cursam nenhum.

Seja T o número de estudantes que cursam pelo menos um curso. Pelo princípio de inclusão-exclusão (Teorema 6.7),

$$T = s_1 - s_2 + s_3 - s_4, \text{ onde}$$
$$s_1 = 12 + 20 + 20 + 8 = 60, \quad s_2 = 5 + 7 + 4 + 16 + 4 + 3 = 39$$
$$s_3 = 3 + 2 + 2 + 3 = 10, \quad s_4 = 2$$

Logo, $T = 29$, e $N = 71 + T = 100$.

6.29 Prove que, se A e B são conjuntos disjuntos finitos, $A \cup B$ é finito e

$$n(A \cup B) = n(A) + n(B)$$

Ao contar os elementos de $A \cup B$, primeiramente conte os de A. Então, existem $n(A)$ destes. Os únicos outros elementos de $A \cup B$ são os que estão em B, mas não em A. Mas como A e B são disjuntos, nenhum elemento de B está em A, e assim existem $n(B)$ elementos que estão em B mas não em A. Portanto, $n(A \cup B) = n(A) + n(B)$.

6.30 Prove o Teorema 6.7 para dois conjuntos: $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

Ao contar os elementos de $A \cup B$, contamos os elementos em A e em B. Existem $n(A)$ em A e $n(B)$ em B. Entretanto, os elementos de A e B foram contados duas vezes. Logo,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

como se queria provar. Para uma outra alternativa de prova, temos as uniões disjuntas:

$$A \cup B = A \cup (B \setminus A) \text{ e } B = (A \cap B) \cup (B \setminus A)$$

Portanto, de acordo com o problema anterior,

$$n(A \cup B) = n(A) + n(B \setminus A) \text{ e } n(B) = n(A \cap B) + n(B \setminus A)$$

Logo, $n(B \setminus A) = n(B) - n(A \cap B)$ e, portanto,

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Como se queria provar.

Problemas Complementares

Notação Fatorial

6.31 Simplifique: (*a*) $\dfrac{(n+1)!}{n!}$; (*b*) $\dfrac{n!}{(n-2)!}$; (*c*) $\dfrac{(n-1)!}{(n+2)!}$; (*d*) $\dfrac{(n-r+1)!}{(n-r-1)!}$.

6.32 Avalie: (*a*) $\binom{5}{2}$; (*b*) $\binom{7}{3}$; (*c*) $\binom{14}{2}$; (*d*) $\binom{6}{4}$; (*e*) $\binom{20}{17}$; (*f*) $\binom{18}{15}$.

Permutações

6.33 Mostre que: (*a*) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n$;

(*b*) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + \binom{n}{n} = 0$.

6.34 (*a*) Quantas placas de carro podem ser feitas se cada uma contiver duas letras distintas seguidas de três algarismos distintos? (*b*) Resolva o problema se o primeiro algarismo não puder ser 0.

6.35 Existem cinco estradas entre *A* e *B* e quatro estradas entre *B* e *C*. Ache o número de caminhos em que se pode dirigir: (*a*) de *A* para *C* passando por *B*; (*b*) fazendo uma rota circular (ida e volta) de *A* para *C* passando por *B*; (*c*) fazendo uma rota circular de *A* para *C* passando por *B*, sem usar a mesma estrada mais de uma vez.

6.36 Ache o número de maneiras pelas quais seis pessoas podem conduzir um tobogã se uma, de um subconjunto de três, tiver de dirigir.

6.37 (*a*) Ache o número de maneiras pelas quais cinco pessoas podem sentar em fila.

(*b*) Quantas serão as maneiras, se duas das pessoas insistirem em sentar em posições contíguas?

(*c*) Resolva a parte (*a*) assumindo que eles se sentem em torno de uma mesa circular.

(*d*) Resolva a parte (*b*) assumindo que eles se sentem em torno de uma mesa circular.

6.38 Ache o número de maneiras em que cinco livros grandes, quatro livros de tamanho médio e três livros pequenos podem ser colocados em uma prateleira, de tal forma que os livros de mesmo tamanho fiquem juntos.

6.39 (*a*) Ache o número de permutações que podem ser formadas com as letras da palavra ELEVEM.

(*b*) Quantas delas começam e terminam com a letra E?

(*c*) Quantas têm os três Es juntos?

(*d*) Quantas começam com E e terminam com M?

6.40 (*a*) De quantas maneiras três meninos e duas meninas podem sentar-se em fila?

(*b*) De quantas maneiras eles podem sentar-se em fila se meninos e meninas tiverem de permanecer agrupados?

(*c*) De quantas maneiras eles podem sentar-se em fila se apenas as meninas tiverem de permanecer agrupadas?

Combinações

6.41 Uma mulher tem 11 amigos próximos.

(*a*) De quantas maneiras ela pode convidar cinco deles para jantar?

(*b*) Quantas são as maneiras, se dois são casados e não comparecerem separadamente?

(*c*) Quantas são as maneiras, se dois deles são brigados e não comparecerem simultaneamente?

6.42 Uma mulher tem 11 amigos próximos dos quais seis também são mulheres.

(*a*) De quantas maneiras ela pode convidar três ou mais para uma festa?

(*b*) De quantas maneiras ela pode convidar três ou mais, se ela quer o mesmo número de homens e mulheres (incluindo ela mesma)?

6.43 Um estudante tem que responder 10 das 13 questões de um exame.

(*a*) Quantas escolhas ele tem?

(*b*) Quantas, se ele deve responder às duas primeiras questões?

(*c*) Quantas, se ele deve responder à primeira ou à segunda questão, mas não a ambas.

(*d*) Quantas, se ele deve responder exatamente a três entre as primeiras cinco questões?

(*e*) Quantas, se ele deve responder a pelo menos três entre as cinco primeiras questões?

Partições

6.44 De quantas maneiras 10 estudantes podem ser divididos em três times, um contendo quatro estudantes, e os outros, três?

6.45 De quantas maneiras 14 pessoas podem ser divididas em seis comitês, em que dois dos comitês contêm três membros, e os outros, dois?

6.46 (*a*) Assumindo que uma célula pode estar vazia, de quantas maneiras um conjunto de três elementos pode ser dividido em (i) três células ordenadas, (ii) três células não ordenadas?

(*b*) De quantas maneiras um conjunto de quatro elementos pode ser dividido em (i) três células ordenadas, (ii) três células não ordenadas?

Problemas Variados

6.47 Uma amostra de 80 proprietários de automóveis revelou que 24 possuíam *vans* e 62 possuíam carros que não eram *vans*. Ache o número k de pessoas que possuem ambos, *vans* e outros tipos de carros.

6.48 Suponha que 12 pessoas leiam o *Wall Street Journal* (W) ou o *Business Week* (B) ou ambos. Sabendo que três pessoas lêem apenas o *Journal* e seis lêem ambos, ache o número k de pessoas que lêem apenas o *Business Week*.

6.49 Mostre que qualquer conjunto de sete inteiros distintos inclui dois inteiros x e y, tais que ou $x + y$ ou $x - y$ seja divisível por 10.

6.50 Considere um torneio em que cada um dos n jogadores joga contra todos os outros e cada jogador ganha pelo menos uma vez. Mostre que existem pelo menos dois jogadores com o mesmo número de vitórias.

Respostas dos Problemas Complementares

6.31 (*a*) $n+1$; (*b*) $n(n-1) = n^2 - n$; (*c*) $1/[n(n+1)(n+2)]$; (*d*) $(n-r)(n-r+1)$.

6.32 (*a*) 10; (*b*) 35; (*c*) 91; (*d*) 15; (*e*) 1140; (*f*) 816.

6.33 *Sugestões:* (*a*) Expanda $(1+1)^n$; (*b*) expanda $(1-1)^n$.

6.34 (*a*) $26 \cdot 25 \cdot 10 \cdot 9 \cdot 8 = 468\,000$; (*b*) $26 \cdot 25 \cdot 9 \cdot 9 \cdot 8 = 421\,200$.

6.35 (*a*) 24; (*b*) 576; (*c*) 360.

6.36 360

6.37 (*a*) 120; (*b*) 48; (*c*) 24; (*d*) 12.

6.38 $3!\,5!\,4!\,3! = 103\,680$.

6.39 (*a*) 120; (*b*) 24; (*c*) 24; (*d*) 12.

6.40 (*a*) 120; (*b*) 24; (*c*) 48.

6.41 (*a*) 462; (*b*) 210; (*c*) 252.

6.42 (*a*) $2^{11} - 1 - \binom{11}{2} - \binom{11}{2} = 1981$ ou $\binom{11}{3} + \binom{11}{4} + \cdots + \binom{11}{11} = 1981$.

(*b*) $\binom{5}{5}\binom{6}{4} + \binom{5}{4}\binom{6}{3} + \binom{5}{3}\binom{6}{2} + \binom{5}{2}\binom{6}{1} = 325$.

6.43 (*a*) 286; (*b*) 165; (*c*) 110; (*d*) 80; (*e*) 276.

6.44 $\dfrac{10!}{4!\,3!\,3!} \cdot \dfrac{1}{2!} = 2100$ ou $\binom{10}{4}\binom{5}{2} = 2100$.

6.45 $\dfrac{14!}{3!\,3!\,2!\,2!\,2!\,2!} \cdot \dfrac{1}{2!\,4!} = 3\,153\,150$.

6.46 (*a*) (i) $3^3 = 27$, cada elemento pode ser colocado em qualquer uma das três células.

(ii) O número de elementos nas três células pode ser distribuído como a seguir:

(*a*) $[\{3\}, \{0\}, \{0\}]$; (*b*) $[\{2\}, \{1\}, \{0\}]$; (*c*) $[\{1\}, \{1\}, \{1\}]$.

Portanto, o número de partições é $1 + 3 + 1 = 5$.

(*b*) (i) $3^4 = 81$.

(ii) O número de elementos nas três células pode ser distribuído como a seguir:

(*a*) $[\{4\}, \{0\}, \{0\}]$; (*b*) $[\{3\}, \{1\}, \{0\}]$; (*c*) $[\{2\}, \{2\}, \{0\}]$; (*d*) $[\{2\}, \{1\}, \{1\}]$.

Portanto, o número de partições é $1 + 4 + 3 + 6 = 14$.

6.47 Pelo Teorema 6.7, $k = 62 + 24 - 80 = 6$.

6.48 Note que $W \cup B = (W \setminus B) \cup (W \cap B) \cup (B \setminus W)$ e a união é disjunta. Portanto, $12 = 3 + 6 + k$ ou $k = 3$.

6.49 Seja $X = \{x_1, x_2, \ldots, x_7\}$ um conjunto de sete inteiros distintos, e seja r_i o resto da divisão de x_i por 10. Considere a seguinte partição de X:

$H_1 = \{x_i : r_i = 0\}$ $\qquad$ $H_2 = \{x_i : r_i = 5\}$

$H_3 = \{x_i : r_i = 1 \text{ ou } 9\}$ $\qquad$ $H_4 = \{x_i : r_i = 2 \text{ ou } 8\}$

$H_5 = \{x_i : r_i = 3 \text{ ou } 7\}$ $\qquad$ $H_6 = \{x_i : r_i = 4 \text{ ou } 6\}$

Existem seis casas de pombos para sete pombos. Se x e y estão em H_1, ou em H_2, então ambos, $x + y$ e $x - y$, são divisíveis por 10. Se x e y estão em um dos outro quatro subconjuntos, então ou $x + y$ ou $x - y$ é divisível por 10, mas não ambos.

6.50 O número de vitórias para cada jogador é pelo menos 1 e, no máximo, $n - 1$. Esses $n - 1$ números correspondem a $n - 1$ casas de pombo que não podem acomodar n jogadores-pombos. Portanto, pelo menos dois jogadores terão o mesmo número de vitórias.

Capítulo 7

Teoria das Probabilidades

7.1 INTRODUÇÃO

Teoria das probabilidades é um tipo de modelagem matemática para fenômenos de azar e aleatoriedade. Se uma moeda é jogada de maneira aleatória, pode-se ter cara ou coroa, mas não sabemos qual deles ocorrerá em um único lance. Entretanto, suponha que s seja o número de vezes que cara aparece quando a moeda é jogada n vezes. À medida que n cresce, a razão $f = s/n$, chamada *freqüência relativa* do resultado, fica mais estável. Se a moeda estiver perfeitamente balanceada, esperamos que caia cara aproximadamente 50% das vezes ou, em outras palavras, que a freqüência relativa se aproxime de $\frac{1}{2}$. De outro ponto de vista, supondo que a moeda seja perfeitamente uniforme, podemos chegar ao valor $\frac{1}{2}$ por dedução. Isto é, é tão provável ocorrer um lado da moeda quanto o outro. Portanto, a chance de se obter cara é de 1 em 2, o que significa que a probabilidade de cara é $\frac{1}{2}$. Embora o resultado específico de um único lance seja desconhecido, o comportamento ao longo de muitas tentativas é determinado. A estabilidade do comportamento de longo prazo de fenômenos aleatórios forma a base da teoria das probabilidades.

Um modelo matemático probabilístico de fenômenos aleatórios é definido associando probabilidades a todos os possíveis resultados de um experimento. A confiabilidade do nosso modelo matemático para um determinado experimento, depende da proximidade entre as probabilidades associadas e o verdadeiro limite das freqüências relativas. Isso origina, então, problemas de verificação e confiabilidade, que são o objeto de estudo da estatística e estão além dos objetivos deste texto.

7.2 ESPAÇO AMOSTRAL E EVENTOS

O conjunto S de todos os possíveis resultados de um experimento é dito o *espaço amostral*. Um resultado particular, i. e., um elemento de S, é dito uma *amostra*. Um *evento* A é um conjunto de resultados ou, em outras palavras, um subconjunto do espaço amostral S. Em particular, o conjunto $\{a\}$ consistindo em uma única amostra $a \in S$ é chamado de *evento elementar*. Ademais, o conjunto vazio, $\varnothing$, e o próprio S são subconjunto de S e, portanto, são eventos. $\varnothing$ é geralmente chamado de *evento impossível* ou *evento nulo*.

Como um evento é um conjunto, podemos combinar eventos para formar novos eventos usando as várias operações entre conjuntos:

(i) $A \cup B$ é o evento que ocorre sse A ocorre *ou* B ocorre (ou ambos).

(ii) $A \cap B$ é o evento que ocorre sse A ocorre e B ocorre.

(iii) A^C, o complementar de A, também representado por $\bar{A}$, é o evento que ocorre sse A *não* ocorre.

Dois eventos A e B são ditos *mutuamente excludentes* se são disjuntos, isto é, se $A \cap B = \emptyset$. Em outras palavras, A e B são mutuamente excludentes sse não podem ocorrer simultaneamente. Três ou mais eventos são mutuamente excludentes se quaisquer dois dentre eles são mutuamente excludentes.

Exemplo 7.1

(*a*) ***Experimento***: Lance um dado e observe o número (de pontos) na face que aparece para cima.
O espaço amostral S consiste em seis números possíveis; isto é,

$$S = \{1, 2, 3, 4, 5, 6\}$$

Seja A o evento descrito pela ocorrência de um número par, B pela ocorrência de um número ímpar e C pela ocorrência de um número primo; isto é, sejam

$$A = \{2, 4, 6\}, \qquad B = \{1, 3, 5\}, \qquad C = \{2, 3, 5\}$$

Então,

$A \cup C = \{2, 3, 4, 5, 6\}$ é o evento ocorrência de um número primo ou par.

$B \cap C = \{3, 5\}$ é o evento ocorrência de um número ímpar primo.

$C^c = \{1, 4, 6\}$ é o evento em que um número primo não ocorre.

Note que A e B são mutuamente excludentes: $A \cap B = \emptyset$. Em outras palavras, um número ímpar e um número par não podem ocorrer simultaneamente.

(*b*) ***Experimento***: Lance uma moeda três vezes e observe a seqüência de ocorrência de caras (H)[1] e coroas (T).
O espaço amostral S consiste nos oito elementos seguintes:

$$S = \{\text{HHH}, \text{HHT}, \text{HTH}, \text{HTT}, \text{THH}, \text{THT}, \text{TTH}, \text{TTT}\}$$

Seja A o evento em que duas ou mais caras aparecem consecutivamente, e B o evento em que todos os lances são iguais; isto é,

$$A = \{\text{HHH}, \text{HHT}, \text{THH}\}. \qquad \text{e} \qquad B = \{\text{HHH}, \text{TTT}\}$$

Então, $A \cap B = \{\text{HHH}\}$ é o evento elementar em que apenas caras aparecem. O evento em que cinco caras aparecem é o conjunto vazio $\emptyset$.

(*b*) ***Experimento***: Lance uma moeda até que uma cara apareça, e então conte o número de vezes que a moeda foi lançada.
O espaço amostral deste experimento é $S = \{1, 2, 3, \ldots\}$. Como todo inteiro positivo é um elemento de S, o espaço amostral é infinito.

Observação: O espaço amostral S no exemplo 7.1(*c*), como observado, não é finito. A teoria que trata desse tipo de espaço amostral está além do escopo deste texto. Portanto, a menos que haja afirmação em contrário, todos os nossos espaços amostrais S serão finitos.

7.3 ESPAÇOS DE PROBABILIDADE FINITOS

Vale a definição a seguir.

Definição: Seja S um espaço amostral finito, $S = \{a_1, a_2, \ldots, a_n\}$. Um *espaço de probabilidade finito*, ou *modelo de probabilidade*, é obtido associando, a cada ponto a_i em S, um número real p_i, chamado de *probabilidade* de a_i, satisfazendo as seguintes propriedades:

(i) Cada p_i é não negativo, isto é, $p_i \geq 0$.

(ii) A soma de p_i é 1, isto é, $p_1 + p_2 + \cdots + p_n = 1$.

A *probabilidade* de um evento A (escreve-se $P(A)$) é então definida como a soma das probabilidades dos pontos em A.

[1] N. de T. Mantivemos, como é comum em textos de probabilidade, os símbolos H para cara (*head*) e T para coroa (*tail*).

O conjunto unitário $\{a_i\}$ é dito um evento *elementar* e, por conveniência de notação, escrevemos $P(a_i)$ em vez de $P(\{a_i\})$.

Exemplo 7.2 *Experimento:* Considere a observação do número de caras obtidas no lançamento de três moedas. [Compare com o Exemplo 7.1(*b*) anterior.]

O espaço amostral é $S = \{0, 1, 2, 3\}$. As seguintes associações aos elementos de S definem um espaço de probabilidades:

$$P(0) = \tfrac{1}{8}, \qquad P(1) = \tfrac{3}{8}, \qquad P(2) = \tfrac{3}{8}, \qquad P(3) = \tfrac{1}{8}$$

Isto é, cada probabilidade é não negativa, e a soma das probabilidades é 1. Seja A o evento em que pelo menos uma cara ocorre, e seja B o evento em que todas as caras ou todas as coroas ocorrem; isto é, seja $A = \{1, 2, 3\}$ e $B = \{0, 3\}$. Então, por definição,

$$P(A) = P(1) + P(2) + P(3) = \tfrac{3}{8} + \tfrac{3}{8} + \tfrac{1}{8} = \tfrac{7}{8} \qquad \text{e} \qquad P(B) = P(0) + P(3) = \tfrac{1}{8} + \tfrac{1}{8} = \tfrac{1}{4}$$

Espaços Equiprováveis

Freqüentemente, as características físicas de um experimento sugerem que probabilidades iguais estão associadas aos vários resultados do espaço amostral. Um tal espaço de probabilidade finito S, onde cada ponto tem a mesma probabilidade, será chamado um *espaço equiprovável*. Em particular, se S contém n pontos, então a probabilidade de cada ponto é $1/n$. Ademais, se um evento A contém r pontos, então sua probabilidade é $r(1/n) = r/n$. Em outras palavras,

$$P(A) = \frac{\text{número de elementos em } A}{\text{número de elementos em } S} = \frac{n(A)}{n(S)} \qquad \text{ou} \qquad P(A) = \frac{\text{número de resultados favoráveis a } A}{\text{número total de resultados possíveis}}$$

onde $n(A)$ denota o número de elementos no conjunto A.
Enfatizamos que a fórmula para $P(A)$ acima só pode ser utilizada em relação a um espaço equiprovável, não podendo ser usada genericamente.

A expressão *aleatório* será usada apenas para referenciar um espaço equiprovável; a declaração "escolha aleatoriamente um ponto de um conjunto S" significará que todo ponto (amostra) em S tem a mesma possibilidade de ser escolhido.

Exemplo 7.3 Considere uma carta selecionada de um baralho comum com 52 cartas. Sejam

$$A = \{\text{a carta é de espadas}\} \quad \text{e} \quad B = \{\text{a carta é uma figura}\}$$

(Uma figura é um valete, uma dama ou um rei.) Computamos $P(A)$ $P(B)$, e $P(A \cap B)$. Como temos um espaço equiprovável,

$$P(A) = \frac{\text{número de espadas}}{\text{número de cartas}} = \frac{13}{52} = \frac{1}{4}, \qquad P(B) = \frac{\text{número de cartas com figura}}{\text{número de cartas}} = \frac{12}{52} = \frac{3}{13}$$

$$P(A \cap B) = \frac{\text{número de cartas de espada com figura}}{\text{número de cartas}} = \frac{3}{32}$$

Teoremas sobre Espaços de Probabilidade Finitos

O teorema seguinte decorre diretamente do fato de que a probabilidade de um evento é a soma das probabilidades dos seus pontos.

Teorema 7-1: A função de probabilidade P definida na classe de todos os eventos em um espaço finito de probabilidades tem as seguintes propriedades:

- $[\mathbf{P}_1]$ Para todo evento A, $0 \le P(A) \le 1$.
- $[\mathbf{P}_2]$ $P(S) = 1$.
- $[\mathbf{P}_3]$ Se os eventos A e B são mutuamente excludentes, então $P(A \cup B) = P(A) + P(B)$.

O próximo teorema formaliza a nossa intuição de que, se p é a probabilidade de um evento E ocorrer, então $1 - p$ é a probabilidade de E não ocorrer. (Isto é, se acertamos um alvo $p = 1/3$ das vezes, então erramos o alvo $1 - p = 2/3$ das vezes.)

Teorema 7-3: seja $\varnothing$ o conjunto vazio, e suponha que A e B são eventos quaisquer. Então:

(i) $P(\varnothing) = 0$
(ii) $P(A \setminus B) = P(A) - P(A \cap B)$
(iii) Se $A \subseteq B$, então $P(A) \leq P(B)$

Observe que a propriedade $[\mathbf{P}_3]$ do Teorema 7.1 indica a probabilidade de união de eventos no caso de eventos disjuntos. A fórmula geral (provada no Problema 7.17) é chamada princípio da adição. Especificamente,

Teorema 7-4 : **(Princípio da Adição)** para quaisquer eventos A e B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Exemplo 7.4 Suponha que um estudante seja aleatoriamente selecionado entre 100 estudantes, dos quais 30 estudam matemática, 20 estudam química e 10 estudam matemática e química. Ache a probabilidade p de um estudante estudar matemática ou química.

Sejam M = {estudantes de matemática} e Q = {estudantes de química}. Como o espaço é equiprovável,

$$P(M) = \frac{30}{100} = \frac{3}{10} \qquad P(Q) = \frac{20}{100} = \frac{1}{5}, \qquad P(M \text{ e } Q) = P(M \cap Q) = \frac{10}{100} = \frac{1}{10}$$

Portanto, pelo Princípio da Adição (Teorema 7.4),

$$p = P(M \text{ or } Q) = P(M \cup Q) = P(M) + P(Q) - P(M \cap Q) = \frac{3}{10} + \frac{1}{5} = \frac{1}{10} = \frac{2}{5}$$

7.4 PROBABILIDADE CONDICIONAL

Suponha que E é um evento em um espaço amostral S com $P(E) > 0$. A probabilidade de um evento A ocorrer uma vez que E tenha ocorrido ou, especificamente, a *probabilidade condicional* de A dado E, (escreve-se $P(A \mid E)$) é definida como a seguir:

$$P(A \mid E) = \frac{P(A \cap E)}{P(E)}$$

$P(A|E)$ mede, em um certo sentido, a probabilidade relativa de A restrita ao espaço reduzido E, como representado no diagrama de Venn da Figura 7-1.

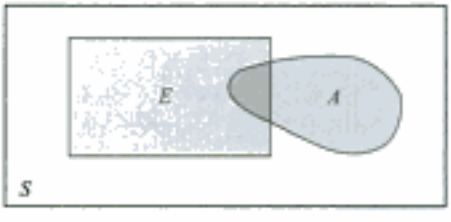


Fig. 7-1

Agora suponha que S é um espaço equiprovável, e seja $n(A)$ o número de elementos no evento A.

$$P(A \cap E) = \frac{n(A \cap E)}{n(S)}, \qquad P(E) = \frac{n(E)}{n(S)}, \qquad \text{e, portanto,} \qquad P(A \mid E) = \frac{P(A \cap E)}{P(E)} = \frac{n(A \cap E)}{n(E)}$$

Afirmamos formalmente esse resultado.

Teorema 7-5: Suponha que S é um espaço equiprovável e que A e B são eventos.

Então

$$P(A \mid E) = \frac{\text{número de elementos em } A \cap E}{\text{número de elementos em } E} = \frac{n(A \cap E)}{n(E)}$$

Exemplo 7.5

(*a*) Um par confiável de dados é lançado. O espaço amostral S consiste em 36 pares ordenados (a, b) onde a e b podem ser quaisquer inteiros entre 1 e 6 (veja o Problema 7.3). Portanto, a probabilidade de qualquer ponto é 1/36. Ache a probabilidade de que um dos dados dê 2, considerando que a soma seja 6. Isto é, ache $P(A \mid E)$ onde

$$E = \{\text{a soma é } 6\} \quad \text{e} \quad A = \{2 \text{ aparece em pelo menos um dos dados}\}.$$

Ache também $P(A)$.

E consiste em cinco elementos, especificamente,

$$E = \{(1,5),\ (2,4),\ (3,3),\ (4,2),\ (5,1)\}$$

Dois deles, (2, 4) e (4, 2), pertencem a A; isto é,

$$A \cap E = \{(2,4),\ (4,2)\}$$

Pelo Teorema 7.5, $P(A \mid E) = 2/5$.

Por outro lado, A consiste em 11 elementos, especificamente,

$$A = \{(2,1),\ (2,2),\ (2,3),\ (2,4),\ (2,5),\ (2,6),\ (1,2),(3,2),\ (4,2),\ (5,2),\ (6,2)\}$$

e S consiste em 36 elementos. Portanto, $P(A) = 11/36$.

(*b*) Um casal tem duas crianças; o espaço amostral é $S = \{hh, hm, mh, mm\}$ com probabilidade 1/4 para cada ponto. Ache a probabilidade p de que ambas as crianças sejam meninos (h) sabendo que: (i) pelo menos uma das crianças é um menino; (ii) a criança mais velha é um menino.

(i) Aqui o espaço restrito consiste em três elementos, $\{hh, hm, mh\}$; logo, $p = \frac{1}{3}$.

(ii) Aqui o espaço restrito consiste em apenas dois elementos $\{hh, hm\}$; logo, $p = \frac{1}{2}$.

Teorema da Multiplicação para Probabilidade Condicional

Suponha que A e B são eventos em um espaço amostral S com $P(A) > 0$. Pela definição de probabilidade condicional,

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$$

Multiplicando ambos os lados por $P(A)$, obtemos o seguinte resultado, bastante útil:

***Teorema 7-6*: (Teorema da multiplicação para probabilidade condicional)**

$$P(A \cap B) = P(A)P(B \mid A)$$

O teorema da multiplicação nos dá uma fórmula para a probabilidade de que ambos os eventos, A e B, ocorram. Ele pode ser facilmente estendido para três ou mais eventos, $A_1, A_2, \ldots A_m$; isto é,

$$P(A_1 \cap A_2 \cap \cdots \cap A_m) = P(A_1) \cdot P(A_2 \mid A_1) \cdot \cdots \cdot P(A_m \mid A_1 \cap A_2 \cap \cdots \cap A_{m-1})$$

Exemplo 7.6 Um lote contém 12 itens, dos quais quatro apresentam defeito. Três itens são aleatoriamente retirados do lote, um após o outro. Ache a probabilidade p de que nenhum dos três apresente defeito.

A probabilidade de o primeiro item não apresentar defeito é $\frac{8}{12}$, já que oito de 12 itens não têm defeitos. Se o primeiro item não tiver defeitos, então a probabilidade de o item seguinte não ter defeitos é $\frac{7}{11}$, já que apenas sete dos

11 itens remanescentes não apresentam defeitos. Se os primeiros dois itens não têm defeitos, então a probabilidade de que o último item não tenha defeitos é $\frac{6}{10}$, já que seis dos 10 itens remanescentes não têm defeitos. Portanto, pelo teorema da multiplicação,

$$p = \frac{8}{12} \cdot \frac{7}{11} \cdot \frac{6}{10} = \frac{14}{55} \approx 0{,}25$$

7.5 EVENTOS INDEPENDENTES

Os eventos A e B em um espaço de probabilidade S são ditos *independentes* se a ocorrência de um deles não influencia a ocorrência do outro. Mais especificamente, B é independente de A se $P(B)$ é igual a $P(B \mid A)$. Agora, substituindo $P(B)$ por $P(B \mid A)$ no teorema da multiplicação, obtém-se

$$P(A \cap B) = P(A)P(B).$$

Usamos formalmente a equação acima como nossa definição de independência de eventos.

Definição: Os eventos A e B são *independentes* se $P(A \cap B) = P(A)P(B)$; caso contrário, eles são *dependentes*.

Enfatizamos que a independência é uma relação de simetria. Em particular, a equação

$$P(A \cap B) = P(A)P(B) \qquad \text{implica tanto} \qquad P(B \mid A) = P(B) \qquad \text{quanto} \qquad P(A \mid B) = P(A)$$

Exemplo 7.7 Uma moeda confiável é lançada três vezes, gerando o espaço equiprovável

$$S = \{\text{HHH}, \text{HHT}, \text{HTH}, \text{HTT}, \text{THH}, \text{THT}, \text{TTH}, \text{TTT}\}$$

Considere os seguintes eventos:

$$A = \{\text{primeiro lance dá cara}\} = \{\text{HHH}, \text{HHT}, \text{HTH}, \text{HTT}\}$$
$$B = \{\text{segundo lance dá cara}\} = \{\text{HHH}, \text{HHT}, \text{THH}, \text{THT}\}$$
$$C = \{\text{exatamente duas caras seguidas}\} = \{\text{HHT}, \text{THH}\}$$

Claramente, A e B são eventos independentes; esse fato é verificado abaixo. Por outro lado, a relação entre A e C ou B e C não é óbvia. Afirmamos que A e C são independentes, mas B e C são dependentes. Temos

$$P(A) = \tfrac{4}{8} = \tfrac{1}{2}, \qquad P(B) = \tfrac{4}{8} = \tfrac{1}{2}, \qquad P(C) = \tfrac{2}{8} = \tfrac{1}{4}$$

Além disso,

$$P(A \cap B) = P(\{\text{HHH}, \text{HHT}\}) = \tfrac{1}{4}, \qquad P(A \cap C) = P(\{\text{HHT}\}) = \tfrac{1}{8}, \qquad P(B \cap C) = P(\{\text{HHT}, \text{THH}\}) = \tfrac{1}{4}$$

Conseqüentemente,

$$P(A)P(B) = \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4} = P(A \cap B), \quad \text{e, logo, } A \text{ e } B \text{ são independentes}$$

$$P(A)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} = P(A \cap C), \quad \text{e, logo, } A \text{ e } C \text{ são independentes}$$

$$P(B)P(C) = \tfrac{1}{2} \cdot \tfrac{1}{4} = \tfrac{1}{8} \neq P(B \cap C), \quad \text{e, logo, } B \text{ e } C \text{ são dependentes}$$

Freqüentemente, postularemos que dois eventos são independentes, ou o próprio experimento implicará que dois eventos sejam independentes.

Exemplo 7.8 A probabilidade de que A atinja um alvo é $\frac{1}{4}$, e a probabilidade de que B atinja um alvo é $\frac{2}{5}$. Ambos atiram no alvo. Ache a probabilidade de que pelo menos um deles atinja o alvo, i.e., A ou B, ou ambos atinjam o alvo.

Temos a informação de que $P(A) = \frac{1}{4}$ e $P(B) = \frac{2}{5}$, e procuramos $P(A \cup B)$. Além disto, a probabilidade de que A ou B atinjam o alvo não é influenciada pela ação do outro, isto é, o evento de A atingir o alvo é independente do evento de B atingir o alvo, isto é, $P(A \cap B) = P(A)P(B)$. Portanto,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = P(A) + P(B) - P(A)P(B) = \tfrac{1}{4} + \tfrac{2}{5} - \left(\tfrac{1}{4}\right)\left(\tfrac{2}{5}\right) = \tfrac{11}{20}$$

7.6 TENTATIVAS INDEPENDENTES REPETIDAS E DISTRIBUIÇÃO BINOMIAL

Discutimos previamente espaços de probabilidade que estavam associados com um experimento repetido finitas vezes, como lançar uma moeda três vezes. O conceito de repetição é formalizado como a seguir:

Definição: Seja S um espaço de probabilidade finita. Designamos, por espaço de *n tentativas independentes repetidas*, o espaço de probabilidade S_n de n-uplas ordenadas de elementos de S, onde a probabilidade de cada n-upla é definida como o produto das probabilidades de seus componentes:

$$P((s_1, s_2, \cdots, s_n)) = P(s_1)P(s_2)\cdots P(s_n)$$

Exemplo 7.9 Sempre que três cavalos, a, b e c, competem, suas respectivas probabilidades de vencer são $\frac{1}{2}$, $\frac{1}{3}$ e $\frac{1}{6}$. Em outras palavras, $S = \{a, b, c\}$ com $P(a) = \frac{1}{2}$, $P(b) = \frac{1}{3}$ e $P(c) = \frac{1}{6}$. Se os cavalos competem duas vezes, o espaço amostral de duas tentativas repetidas é

$$S_2 = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$$

Por conveniência de notação, escrevemos ac para o par ordenado (a, c). A probabilidade de cada ponto em S_2 é

$$\begin{aligned}
P(aa) &= P(a)P(a) = \tfrac{1}{2}\left(\tfrac{1}{2}\right) = \tfrac{1}{4}, & P(ba) &= \tfrac{1}{6}, & P(ca) &= \tfrac{1}{12}\\
P(ab) &= P(a)P(b) = \tfrac{1}{2}\left(\tfrac{1}{3}\right) = \tfrac{1}{6}, & P(bb) &= \tfrac{1}{9}, & P(cb) &= \tfrac{1}{18}\\
P(ac) &= P(a)P(c) = \tfrac{1}{2}\left(\tfrac{1}{6}\right) = \tfrac{1}{12}, & P(bc) &= \tfrac{1}{18}, & P(cc) &= \tfrac{1}{36}
\end{aligned}$$

Portanto, a probabilidade de c ganhar o primeiro páreo e a ganhar o segundo é $P(ca) = \frac{1}{12}$.

Tentativas Repetidas com dois Resultados, Tentativas de Bernoulli

Considere um experimento com apenas dois resultados possíveis. Tentativas independentes repetidas de um tal experimento são chamadas de tentativas de Bernoulli, em homenagem ao matemático suíço Jacob Bernoulli (1654–1705). O termo "tentativas independentes" significa que o resultado de qualquer tentativa não depende do resultado de tentativas prévias (tal como lançar uma moeda). Chamaremos um dos resultados de *sucesso* e o outro de *fracasso*.

Seja p a probabilidade de sucesso em uma tentativa de Bernoulli; logo, $q = 1 - p$ é a probabilidade de um fracasso. Um *experimento binomial* consiste em um número fixo de tentativas de Bernoulli. A notação

$$B(n, p)$$

será usada para denotar um experimento binomial com n tentativas e probabilidade p de sucesso.

Freqüentemente, estamos interessados no número de sucessos em um experimento binomial, e não na ordem em que ocorrem. O seguinte teorema (provado no Problema 7.38) pode ser usado.

Teorema 7-7: a probabilidade de se obter exatamente k sucessos em um experimento binomial $B(n, p)$ é dada por

$$P(k) = P(k \text{ sucesso}) = \binom{n}{k} p^k q^{n-k}$$

A probabilidade de um ou mais sucessos é $1 - q^n$.

Aqui, $\binom{n}{k}$ é o coeficiente binomial, que está definido e discutido no Capítulo 6.

Exemplo 7.10 Uma moeda confiável é lançada seis vezes; considere a obtenção de caras como sucesso. Este é um experimento binomial com $n = 6$ e $p = q = \frac{1}{2}$.

(*a*) A probabilidade de que exatamente duas caras ocorram (i.e., $k = 2$) é

$$P(2) = \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{15}{64} \approx 0{,}23$$

(*b*) A probabilidade de se obterem pelo menos quatro caras (i.e., $k = 4$, 5 ou 6) é

$$P(4) + P(5) + P(6) = \binom{6}{4}\left(\frac{1}{2}\right)^4\left(\frac{1}{2}\right)^2 + \binom{6}{5}\left(\frac{1}{2}\right)^5\left(\frac{1}{2}\right) + \binom{6}{6}\left(\frac{1}{2}\right)^6$$
$$= \frac{15}{64} + \frac{6}{64} + \frac{1}{64} = \frac{11}{32} \approx 0{,}34$$

(*c*) A probabilidade de não se obter nenhuma cara (i.e., apenas fracassos) é $q^6 = \left(\frac{1}{2}\right)^6 = \frac{1}{64}$; logo, a probabilidade de uma ou mais caras é $1 - q^n = 1 - \frac{1}{64} = \frac{63}{64} \approx 0{,}94$.

Observação: A função $P(k)$ para $k = 1,2,\ldots, n$, para um experimento binomial $B(n, p)$, é dita a *distribuição binomial*, já que corresponde aos termos sucessivos da expansão binomial:

$$(q + p)^n = q^n + \binom{n}{1}q^{n-1}p + \binom{n}{2}q^{n-2}p^2 + \cdots + p^n$$

O uso do termo *distribuição* será explicado adiante neste capítulo.

7.7 VARIÁVEIS ALEATÓRIAS

Seja S uma amostra de um experimento. Como observado previamente, o resultado de um experimento, ou os pontos em S, não precisam ser números. Por exemplo, no lançamento de uma moeda, os resultados são cara (H) ou coroa (T), e no lançamento de um par de dados, os resultados são um par de inteiros. Entretanto, freqüentemente queremos associar um número específico a cada resultado do experimento. Por exemplo, no lançamento de moedas, pode ser conveniente associar 1 a H e 0 a T; ou, no lançamento de um par de dados, podemos querer associar a soma dos dois inteiros ao resultado. Uma associação de valores numéricos desse tipo é chamada *variável aleatória*. Mais genericalmente, temos a definição seguinte.

Definição: Uma *variável aleatória* X é uma regra que associa um valor numérico a cada resultado de um espaço amostral S.

Vamos denotar por R_X[†] o conjunto de números associados por uma variável aleatória X, e vamos nos referir a R_X como *espaço imagem*.

Observação: Em uma terminologia mais formal, X é uma função de S para os números reais $\mathbf{R}$, e R_X é a imagem de X. Além disso, para alguns espaços amostrais infinitos S, nem todas as funções de S para $\mathbf{R}$ são consideradas variáveis aleatórias. Entretanto, os espaços amostrais aqui são finitos, e toda função a valores reais definida em um espaço amostral finito é uma variável aleatória.

Exemplo 7.11 Um par de dados confiáveis é lançado (veja o Problema 7.3). O espaço amostral S consiste em 36 pares ordenados (a, b) onde a e b podem ser n inteiros entre 1 e 6; isto é,

$$S = \{(1,1),\ (1,2), \ldots, (6,6)\}$$

Suponha que X associa a soma dos números a cada ponto em S; então X é uma variável aleatória com espaço imagem

$$R_X = \{2,3,4,5,6,7,8,9,10,11,12\}$$

Suponha que Y associa a cada ponto o máximo de dois números; então Y é uma variável aleatória com espaço imagem

$$R_Y = \{1,2,3,4,5,6\}$$

Exemplo 7.12 Uma caixa contém 12 itens dos quais três são defeituosos. Uma amostra de três itens é selecionada da caixa. O espaço amostral consiste em $\binom{12}{3} = 220$ amostras diferentes de tamanho 3. Seja X o número de itens defeituosos na amostra; então X é uma variável aleatória com espaço imagem $R_X = \{0,1,2,3\}$.

[†] N. de T. Como nos capítulos anteriores, a letra R é usada como símbolo para imagem (em inglês, *range*).

Distribuição de Probabilidade de uma Variável Aleatória

Seja $R_X = \{x_1, x_2, \ldots, x_t\}$ o espaço imagem de uma variável aleatória X definida em um espaço amostral finito S. Então X induz uma associação de probabilidades no espaço imagem R_X como a seguir:

$$p_i = P(x_i) = P(X = x_i) = \text{soma das probabilidades dos pontos em } S \text{ cuja imagem é } x_i.$$

O conjunto dos pares ordenados $(x_1, p_1), \ldots, (x_t, p_t)$, normalmente dado por uma tabela

x_1	x_2	$\cdots$	x_t
p_1	p_2	$\cdots$	p_t

é dito a *distribuição* da variável aleatória X.

No caso em que S é um espaço equiprovável, podemos facilmente obter a distribuição de uma variável aleatória como a seguir.

Teorema 7-8: seja S um espaço equiprovável, e seja X uma variável aleatória em S com espaço imagem

$$R_X = \{x_1, x_2, \ldots, x_t\}.$$

Então,

$$p_i = P(x_i) = \frac{\text{número de pontos em } S \text{ cuja imagem é } x_i}{\text{número de pontos em } S}$$

Exemplo 7.13 Considere a variável aleatória X do Exemplo 7.11 que associa, ao lançamento de um par de dados, a soma dos valores. Usamos o Teorema 7.8 para obter a distribuição de X.

Existe apenas um resultado (1, 1) cuja soma é 2; portanto, $P(2) = \frac{1}{36}$. Existem dois resultados, (1, 2) e (2, 1), cuja soma é 3; portanto, $P(3) = \frac{2}{36}$. Existem três resultados, (1, 3), (2, 2) e (3, 1), cuja soma é 4; portanto $P(4) = \frac{3}{36}$. De modo similar, $P(5) = \frac{4}{36}$, $P(6) = \frac{5}{36}, \ldots, P(12) = \frac{1}{36}$. A distribuição de X consiste nos pontos em R_X com suas respectivas probabilidades; isto é,

x_i	2	3	4	5	6	7	8	9	10	11	12
p_i	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Exemplo 7.14 Seja X a variável aleatória do Exemplo 7.12. Usamos o Teorema 7.8 para obter a distribuição de X.

Existem $\binom{9}{3} = 84$ amostras de tamanho 3 sem itens defeituosos; portanto, $P(0) = \frac{84}{220}$. Existem $3\binom{9}{2} = 108$ amostras de tamanho 3 contendo um item defeituoso; portanto, $P(1) = \frac{108}{220}$. Existem $\binom{3}{2} \cdot 9 = 27$ amostras de tamanho 3 contendo dois itens defeituosos; portanto, $P(2) = \frac{27}{220}$. Existe apenas uma amostra de tamanho 3 contendo três itens defeituosos; portanto $P(3) = \frac{1}{220}$. A distribuição de X é a seguinte:

x_i	0	1	2	3
p_i	$\frac{84}{220}$	$\frac{108}{220}$	$\frac{27}{220}$	$\frac{1}{220}$

Observação: Seja X uma variável aleatória em um espaço de probabilidade $S = \{a_1, a_2, \ldots, a_m\}$, e seja $f(x)$ um polinômio qualquer. Então, $f(X)$ é a variável aleatória que associa $f(X(a_i))$ ao ponto a_i ou, em outras palavras, $f(X)(a_i) = f(X(a_i))$. Conseqüentemente, se X assume os valores $x_1, x_2, \ldots, x_n$, com as respectivas probabilidades $p_1, p_2, \ldots, p_n$, então $f(X)$ assume os valores $f(x_1), f(x_2), \ldots, f(x_n)$, onde a probabilidade q_k de y_k é a soma dos valores p_i para os quais $y_k = f(x_i)$.

Expectância de uma Variável Aleatória

Seja X uma variável aleatória. Existem duas medidas (ou parâmetros) importantes associados a X: a *média* de X, denotada por μ ou μ_X, e o *desvio-padrão* de X, denotado por σ ou σ_X. A média μ é também chamada de *expectância* de X, escrita $E(X)$. Em um certo sentido, a média μ mede a "tendência central" de X, e o desvio-padrão σ mede o "espalhamento" ou "dispersão" de X. Esta subseção discute a expectância $\mu = E(X)$ de X, e a subseção seguinte discute o desvio-padrão σ de X.

Seja X uma variável aleatória em um espaço de probabilidade $S = \{a_1, a_2, \cdots, a_m\}$. A *média* ou *expectância* de X é definida por

$$\mu = E(X) = X(a_1)P(a_1) + X(a_2)P(a_2) + \cdots + X(a_m)P(a_m) = \Sigma X(a_i)P(a_i)$$

Em particular, se X é dado pela distribuição

x_1	x_2	$\cdots$	x_n
p_1	p_2	$\cdots$	p_n

então a *expectância* de X é

$$\mu = E(X) = x_1p_1 + x_2p_2 + \cdots + x_np_n = \Sigma x_ip_i$$

(Por conveniência de notação, omitimos os limites no símbolo de somatório Σ.)

Exemplo 7.15

(*a*) Suponha que uma moeda confiável seja lançada seis vezes. O número de caras que podem ocorrer, com as respectivas probabilidades, é o seguinte:

x_i	0	1	2	3	4	5	6
p_i	$\frac{1}{64}$	$\frac{6}{64}$	$\frac{15}{64}$	$\frac{20}{64}$	$\frac{15}{64}$	$\frac{6}{64}$	$\frac{1}{64}$

Então a média, ou expectância, ou número esperado de caras, é

$$\mu = E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{6}{64}\right) + 2\left(\tfrac{15}{64}\right) + 3\left(\tfrac{20}{64}\right) + 4\left(\tfrac{15}{64}\right) + 5\left(\tfrac{6}{64}\right) + 6\left(\tfrac{1}{64}\right) = 3$$

(*b*) Considere a variável aleatória X do Exemplo 7.12 cuja distribuição aparece no Exemplo 7.14. Ela informa o número possível de itens defeituosos em uma amostra de tamanho 3 com suas respectivas probabilidades. Então, a expectância de X ou, em outras palavras, o número esperado de itens defeituosos em uma amostra de tamanho 3 é

$$\mu = E(X) = 0\left(\tfrac{84}{220}\right) + 1\left(\tfrac{108}{220}\right) + 2\left(\tfrac{27}{220}\right) + 3\left(\tfrac{1}{220}\right) = 0{,}75$$

(*c*) Três cavalos, a, b e c, estão em um páreo; suponha que as suas respectivas probabilidades de vitória sejam $\frac{1}{2}$, $\frac{1}{3}$ e $\frac{1}{6}$. Seja X a função que descreve o pagamento do prêmio para o cavalo vencedor, e suponha que X pague \$ 2, \$ 6 ou \$ 9, dependendo de a, b ou c vencer o páreo. O pagamento esperado para o páreo é

$$\begin{aligned} E(X) &= X(a)P(a) + X(b)P(b) + X(c)P(c) \\ &= 2\left(\tfrac{1}{2}\right) + 6\left(\tfrac{1}{3}\right) + 9\left(\tfrac{1}{6}\right) = 4{,}5 \end{aligned}$$

Variância e Desvio-Padrão de uma Variável Aleatória

Considere uma variável aleatória X com média μ e distribuição de probabilidade

x_1	x_2	x_3	$\cdots$	x_n
p_1	p_2	p_3	$\cdots$	p_n

A *variância* $\text{Var}(X)$ e o *desvio-padrão* σ de X são definidos por

$$\text{Var}(X) = (x_1 - \mu)^2 p_1 + (x_2 - \mu)^2 p_2 + \cdots + (x_n - \mu)^2 p_n = \Sigma (x_i - \mu)^2 p_i = E((X - \mu)^2)$$
$$\sigma = \sqrt{\text{Var}(X)}$$

A seguinte fórmula é, normalmente, mais conveniente do que a fórmula acima para calcular $\text{Var}(X)$:

$$\text{Var}(X) = x_1^2 p_1 + x_2^2 p_2 + \cdots + x_n^2 p_n - \mu^2 = \Sigma x_i^2 p_i - \mu^2 = E(X^2) - \mu^2$$

Observação: De acordo com a fórmula acima, $\text{Var}(X) = \sigma^2$. Tanto, σ^2 quanto σ medem o espalhamento ponderado dos valores x_i em torno da média μ; entretanto, σ tem as mesmas unidades que μ.

Exemplo 7.16

(*a*) Seja X o número ocorrências de cara quando uma moeda confiável é lançada seis vezes. A distribuição de X aparece no Exemplo 7.15(*a*), onde a sua média $\mu = 3$ é calculada. A variância de X é calculada como a seguir:

$$\text{Var}(X) = (0-3)^2 \tfrac{1}{64} + (1-3)^2 \tfrac{6}{64} + (2-3)^2 \tfrac{15}{64} + \cdots + (6-3) \tfrac{1}{64} = 1{,}5$$

De outra maneira,

$$\text{Var}(X) = 0^2 \tfrac{1}{64} + 1^2 \tfrac{6}{64} + 2^2 \tfrac{15}{64} + 3^2 \tfrac{20}{64} + 4^2 \tfrac{15}{64} + 5^2 \tfrac{6}{64} + 6^2 \tfrac{1}{64} - 3^2 = 1{,}5$$

O desvio-padrão é $\sigma = \sqrt{1{,}5} \approx 1{,}225$ (caras).

(*b*) Considere a variável aleatória X no exemplo 7.15(*b*), onde a sua média $\mu = 0{,}75$ é calculada. (A distribuição aparece no Exemplo 7.14.) A variância de X é calculada como a seguir:

$$\text{Var}(X) = 0^2 \tfrac{84}{220} + 1^2 \tfrac{108}{220} + 2^2 \tfrac{27}{220} + 3^2 \tfrac{1}{220} - (0{,}75)^2 = 0{,}46$$

Portanto, o desvio-padrão é

$$\sigma = \sqrt{\text{Var}(X)} = \sqrt{0{,}46} = 0{,}66$$

Distribuição Binomial

Considere um experimento binomial $B(n, p)$. Isto é, $B(n, p)$ consiste em n repetições de um experimento com dois resultados possíveis, sucesso ou fracasso, e p é a probabilidade de sucesso. O número X de k sucessos é uma variável aleatória cuja distribuição aparece na Figura 7-2.

k	0	1	2	$\cdots$	n
$P(k)$	q^n	$\binom{n}{1} q^{n-1} p$	$\binom{n}{2} q^{n-2} p^2$	$\cdots$	p^n

Fig. 7-2

O teorema seguinte pode ser usado.

Teorema 7-9: considere a distribuição binomial $B(n, p)$. Então:

(i) Valor esperado $E(X) = \mu = np$

(ii) Variância $\text{Var}(X) = \sigma^2 = npq$

(iv) Desvio-padrão $\sigma = \sqrt{npq}$

Exemplo 7.17

(*a*) A probabilidade de um homem atingir um alvo é $p = 1/5$. Ele atira 100 vezes. Ache o número esperado μ de vezes que ele vai atingir o alvo e o desvio-padrão σ.

Aqui $p = \frac{1}{5}$ e, logo, $q = \frac{4}{5}$. Portanto,

$$\mu = np = 100 \cdot \frac{1}{5} = 20 \qquad \text{e} \qquad \sigma = \sqrt{npq} = \sqrt{100 \cdot \frac{1}{5} \cdot \frac{4}{5}} = 4$$

(*b*) Ache o número esperado de respostas corretas obtidas por adivinhação em um teste com cinco questões do tipo falso ou verdadeiro.

Aqui, $p = \frac{1}{2}$. Portanto, $E(X) = np = 5 \cdot \frac{1}{2} = 2.5$.

Problemas Resolvidos

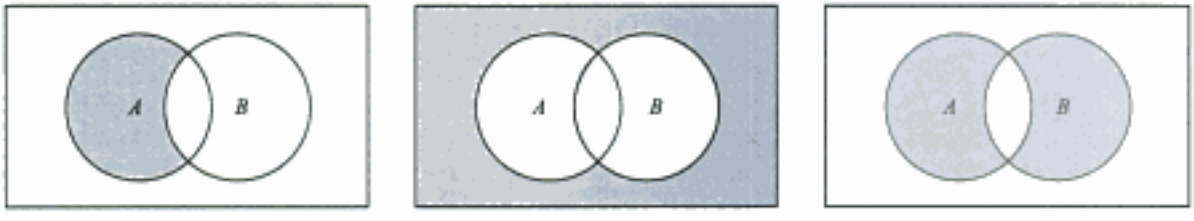
Espaços Amostrais e Eventos

7.1 Sejam A e B eventos. Ache uma expressão e exiba o diagrama de Venn para os eventos: (*a*) A, mas não B; (*b*) nem A nem B; (*c*) A ou B, mas não ambos.

(*a*) Como A mas não B ocorre, assinale a área de A fora de B, como na Figura 7-3(*a*). Note que B^c, o complementar de B, ocorre, já que B não ocorre; portanto, A e B^c ocorrem. Em outras palavras, o evento é $A \cap B^c$.

(*b*) "Nem A nem B" significa que "não A e não B" ou $A^c \cap B^c$. Pela lei de DeMorgan, isto também é $(A \cup B)^c$; portanto, assinale a área fora de A e B, i.e., fora de $A \cup B$, como na Figura 7-3(*b*).

(*c*) Como A ou B mas não ambos ocorre, assinale a área de A e B, exceto a sua interseção, como na Figura 7-3(*c*). O evento é equivalente à ocorrência de A mas não B ou B mas não A. Portanto, o evento é $(A \cap B^c) \cup (B \cap A^c)$.



(*a*) A mas não B (*b*) Nem A nem B (*c*) A ou B, mas não ambos

Fig. 7-3

7.2 Considere o lançamento de um dado e de uma moeda; seja S o espaço amostral consistindo nos 12 elementos:

$$S = \{\text{H1, H2, H3, H4, H5, H6, T1, T2, T3, T4, T5, T6}\}$$

(*a*) Expresse explicitamente os seguintes eventos:

$A = \{\text{cara e um número ímpar aparecem}\}$

$B = \{\text{ um número primo aparece}\}$

$C = \{\text{coroa e um número ímpar aparecem}\}$

(*b*) Expresse explicitamente os eventos: (i) A ou B ocorre; (ii) B e C ocorrem; (iii) apenas B ocorre.

(*c*) Qual par formado a partir dos eventos A, B e C é composto de eventos mutuamente exclusivos?

(*a*) Os elementos de A são os elementos de S consistindo em um H e um número par:

$$A = \{\text{H2, H4, H6}\}$$

Os elementos de B são os pontos em S cujo segundo componente é um número primo:

$$B = \{\text{H2, H3, H5, T2, T3, T5}\}$$

Os elementos de C são os pontos de S formados por um T e um número ímpar: $C = \{\text{T1, T3, T5}\}$.

(*b*) (i) $A \cup B = \{H2, H4, H6, H3, H5, T2, T3, T5\}$.

(ii) $B \cap C = \{T3, T5\}$.

(iii) $B \cap A^c \cap C^c = \{H3, H5, T2\}$.

(*c*) A e C são mutuamente excludentes, já que $A \cap C = \varnothing$.

7.3 Um par de dados é lançado e os dois números são registrados. Escreva o espaço amostral S, e ache o número $n(S)$ de elementos em S.

Existem seis números possíveis, 1, 2,..., 6, em cada dado. Portanto, $n(S) = 6 \cdot 6 = 36$, e S consiste em 36 pares de números de 1 a 6. A Figura 7-4 mostra esses 36 pares em um *array* em que cada linha tem os primeiros elementos iguais e cada coluna tem os segundos elementos iguais.

(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6)
(2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 6)
(3, 1), (3, 2), (3, 3), (3, 4), (3, 5), (3, 6)
(4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (4, 6)
(5, 1), (5, 2), (5, 3), (5, 4), (5, 5), (5, 6)
(6, 1), (6, 2), (6, 3), (6, 4), (6, 5), (6, 6)

Fig. 7-4

7.4 Considere o espaço amostral S do Problema 7.3. Ache o número de elementos em cada um dos seguintes eventos:

(*a*) A = {os dois números são iguais}.

(*b*) B = {a soma é 10 ou mais}.

(*c*) C = {5 aparece no primeiro dado}.

(*d*) D = {5 aparece em pelo menos um dado}.

(*e*) E = {a soma é 7 ou menos}.

Use a Figura 7-4 para ajudar a contar o número de elementos que estão no evento:

(*a*) $A = \{(1,1), (2,2), \ldots, (6,6)\}$; logo, $n(A) = 6$.

(*b*) $B = \{(6,4), (5,5), (4,6), (6,5), (5,6), (6,6)\}$; logo, $n(B) = 6$.

(*c*) $C = \{(5,1), (5,2), \ldots, (5,6)\}$; logo, $n(C) = 6$.

(*d*) Existem seis pares tendo 5 como primeiro elemento e seis pares com 5 como segundo elemento. Entretanto, (5,5) aparece em ambas as situações. Portanto,

$$n(D) = 6 + 6 - 1 = 11$$

Como outra alternativa de resolução, conte os pares da Figura 7-4 que estão em D para obter $n(D) = 11$.

(*e*) Seja $n(s)$ o número de pares em S cuja soma é s. A soma 7 aparece na diagonal do *array* na Figura 7-4; portanto, $n(7) = 6$. A soma 6 aparece imediatamente abaixo da diagonal logo, $n(6) = 5$. De modo semelhante, $n(5) = 4$, $n(4) = 3$, $n(3) = 2$, e $n(2) = 1$. Logo,

$$n(S) = 6 + 5 + 4 + 3 + 2 + 1 = 21$$

Como outra opção para a resolução, $n(7) = 6$, e existem $36 - 6 = 30$ pares remanescentes. Metade deles tem somas excedendo a 7, e metade tem soma menor do que 7. Logo, $n(s) = 6 + 15 = 21$.

Espaços Equiprováveis Finitos

7.5 Determine a probabilidade p de cada evento.

(*a*) Um número ímpar aparece no lançamento de um dado confiável.

(*b*) Uma ou mais caras aparecem no lançamento de três moedas confiáveis.

(*c*) Uma bola de gude vermelha é retirada aleatoriamente de uma caixa contendo quatro bolas brancas, três vermelhas e cinco azuis.

Cada espaço amostral S é um espaço equiprovável. Portanto, para cada evento E, use

$$P(E) = \frac{\text{número de elementos em } E}{\text{número de elementos em } S} = \frac{n(E)}{n(S)}$$

(*a*) O evento pode ocorrer de três maneiras (2,4 ou 6) dentre seis possibilidades; logo, $p = \frac{3}{6} = \frac{1}{2}$.

(*b*) Assumindo que as moedas sejam distintas, existem oito casos:

$$\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}$$

Apenas o último caso não é favorável; portanto, $p = 7/8$.

(*c*) Existem $4 + 3 + 5 = 12$ bolas de gude das quais três são vermelhas; portanto, $p = \frac{3}{12} = \frac{1}{4}$.

7.6 Uma carta é retirada de um baralho comum S de 52 cartas. Ache a probabilidade p de:

(*a*) A carta ser um rei.

(*b*) A carta ser uma figura (valete, dama ou rei).

(*c*) A carta ser de copas.

(*d*) A carta ser uma figura de copas.

(*e*) A carta ser uma figura ou ser de copas.

Aqui, $n(S) = 52$.

(*a*) Existem quatro reis; portanto, $p = \frac{4}{52} = \frac{1}{13}$.

(*b*) Existem $4(3) = 12$ figuras; portanto, $p = \frac{12}{52} = \frac{3}{13}$.

(*c*) Existem 13 cartas de copas; portanto, $p = \frac{13}{52} = \frac{1}{4}$.

(*d*) Existem três figuras de copas; portanto, $p = \frac{3}{52}$.

(*e*) Tomando $F = \{\text{figuras}\}$ e $C = \{\text{copas}\}$, temos

$$n(F \cup C) = n(F) + n(C) - n(F \cap C) = 12 + 13 - 3 = 22$$

Portanto, $p = \frac{22}{52} = \frac{11}{26}$.

7.7 Considere o espaço amostral S do Problema 7.2. Assuma que uma moeda e um dado são confiáveis; logo, S é um espaço equiprovável. Ache: (*a*) $P(A)$, $P(B)$, $P(C)$; (*b*) $P(A \cup B)$, $P(B \cap C)$, $P(B \cap A^c \cap C^c)$.

Como S é um espaço equiprovável, use $P(E) = n(E)/n(S)$. Aqui, $n(S) = 12$. Logo, precisamos apenas contar o número de elementos no conjunto dado.

(*a*) $P(A) = \frac{3}{12}$, $P(B) = \frac{6}{12}$, $P(C) = \frac{3}{12}$.

(*b*) $P(A \cup B) = \frac{8}{12}$, $P(B \cap C) = \frac{2}{12}$, $P(B \cap A^c \cap C^c) = \frac{3}{12}$.

7.8 Duas cartas são retiradas aleatoriamente de um baralho comum de 52 cartas. Ache a probabilidade p de que: (*a*) ambas sejam de espadas; (*b*) uma seja de espada e a outra, de copas.

Existem $\binom{52}{2} = 1.326$ maneiras de retirar duas dentre 52 cartas.

(*a*) Existem $\binom{13}{2} = 78$ maneiras de retirar duas cartas de espadas de 13 espadas; portanto,

$$p = \frac{\text{número de maneiras com que duas espadas podem ser retiradas}}{\text{número de maneiras com que duas cartas podem ser retiradas}} = \frac{78}{1.326} = \frac{3}{51}$$

(*b*) Existem 13 espadas e 13 copas; portanto, existem $13 \cdot 13 = 169$ maneiras de retirar uma carta de espadas e uma de copas. Logo, $p = \frac{169}{1.326} = \frac{13}{102}$.

7.9 Uma caixa contém duas meias brancas e duas meias azuis. Duas meias são retiradas aleatoriamente. Ache a probabilidade p de que elas combinem (sejam da mesma cor).

Existem $\binom{4}{2} = 6$ maneiras de retirar duas das meias. Apenas dois pares levarão a uma combinação. Portanto, $p = \frac{2}{6} = \frac{1}{3}$.

7.10 Cinco cavalos estão em um páreo. Adriana escolhe aleatoriamente dois dos cavalos e aposta neles. Ache a probabilidade p de que Adriana tenha escolhido o vencedor.

Existem $\binom{5}{2} = 10$ maneiras de escolher dois dos cavalos. Quatro dos pares irão conter o vencedor. Portanto, $p = \frac{4}{10} = \frac{2}{5}$.

Espaços de Probabilidade Finita

7.11 Um espaço amostral S consiste em quatro elementos; isto é, $S = \{a_1, a_2, a_3, a_4\}$. Munido de quais das seguintes funções S se torna um espaço de probabilidade?

(*a*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{3}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = \frac{1}{5}$
(*b*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = -\frac{1}{4}$ $P(a_4) = \frac{1}{2}$
(*c*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{8}$ $P(a_4) = \frac{1}{8}$
(*d*) $P(a_1) = \frac{1}{2}$ $P(a_2) = \frac{1}{4}$ $P(a_3) = \frac{1}{4}$ $P(a_4) = 0$

(*a*) Como a soma dos valores nas amostras é maior do que 1, a função não define S como um espaço de probabilidade.
(*b*) Como $P(a_3)$ é negativo, a função não define S como um espaço de probabilidade.
(*c*) Como cada valor é não negativo e a soma dos valores é 1, a função define S como um espaço de probabilidade.
(*d*) Os valores são não negativos e somam 1; logo, a função define S como um espaço de probabilidade.

7.12 Uma moeda tem uma distribuição de peso tal que é duas vezes mais provável aparecer cara do que coroa. Ache $P(T)$ e $P(H)$.

Seja $P(T) = p$; então, $P(H) = 2p$. Agora iguale a soma das probabilidades a 1, isto é, $p + 2p = 1$. Então, $p = \frac{1}{3}$. Portanto, $P(H) = \frac{1}{3}$ e $P(T) = \frac{2}{3}$.

7.13 Um dado é balanceado de tal maneira que os resultados produzem a seguinte distribuição de probabilidades:

Resultado	1	2	3	4	5	6
Probabilidade	0,1	0,3	0,2	0,1	0,1	0,2

Considere os eventos:

$A = \{\text{número par}\}$, $B = \{2, 3, 4, 5\}$, $C = \{x: x < 3\}$, $D = \{x: x > 7\}$

Ache as seguintes probabilidades:

(*a*) (i) $P(A)$, (ii) $P(B)$, (iii) $P(C)$, (iv) $P(D)$.
(*b*) $P(A^c)$, $P(B^c)$, $P(C^c)$, $P(D^c)$.
(*c*) (i) $P(A \cap B)$, (ii) $P(A \cup C)$, (iii) $P(B \cap C)$.

(*a*) Para qualquer evento, ache $P(E)$ somando as probabilidades dos elementos em E. Logo:
(i) $A = \{2, 4, 6\}$; logo, $P(A) = 0{,}3 + 0{,}1 + 0{,}2 = 0{,}6$.
(ii) $P(B) = 0{,}3 + 0{,}2 + 0{,}1 + 0{,}1 = 0{,}7$.
(iii) $C = \{1, 2\}$; logo, $P(C) = 0{,}1 + 0{,}3 = 0{,}4$.
(iv) $D = \varnothing$, o conjunto vazio. Logo, $P(D) = 0$.

(*b*) Use $P(E^c) = 1 - P(E)$ para obter:

$$P(A^c) = 1 - 0{,}6 = 0{,}4, \qquad P(C^c) = 1 - 0{,}4 = 0{,}6$$
$$P(B^c) = 1 - 0{,}7 = 0{,}3, \qquad P(D^c) = 1 - 0 = 1$$

(*c*) (i) $A \cap B = \{2, 4\}$; logo, $P(A \cap B) = 0{,}3 + 0{,}1 = 0{,}4$.
(ii) $A \cup C = \{1, 2, 3, 4, 5\} = \{6\}^c$; logo, $P(A \cup C) = 1 - 0{,}2 = 0{,}8$.
(iii) $B \cap C = \{2\}$; logo, $P(B \cap C) = 0{,}3$.

7.14 Suponha que A e B são eventos com $P(A) = 0{,}6$, $P(B) = 0{,}3$ e $P(A \cap B) = 0{,}2$. Ache a probabilidade de:

(*a*) A não ocorrer.
(*b*) B não ocorrer.
(*c*) A ou B ocorrerem.
(*d*) Nem A nem B ocorrerem.

(*a*) $P(\text{não } A) = P(A^c) = 1 - P(A) = 0{,}4$.

(*b*) $P(\text{não } B) = P(B^c) = 1 - P(B) = 0{,}7$.

(*c*) Pelo princípio da adição,

$$P(A \text{ ou } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B)$$
$$= 0{,}6 + 0{,}3 - 0{,}2 = 0{,}7$$

(*d*) Relembre [Figura 7-3(*b*)] que "nem A nem B" é o complementar de $A \cup B$. Portanto,

$$P(\text{nem } A \text{ nem } B) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0{,}7 = 0{,}3$$

7.15 Prove o Teorema 7.2: $P(A^c) = 1 - P(A)$.

$S = A \cup A^C$, onde A e A^C são disjuntos. Portanto,

$$1 = P(S) = P(A \cup A^c) = P(A) + P(A^c)$$

de onde segue o resultado.

7.16 Prove o Teorema 7.3: (i) $P(\varnothing) = 0$, (ii) $P(A \setminus B) = P(A) - P(A \cap B)$, (iii) Se $A \subseteq B$, então $P(A) < P(B)$.

(i) $\varnothing = S^c$ e $P(S) = 1$. Logo, $P(\varnothing) = 1 - 1 = 0$.

(ii) Como indicado na Figura 7-5(*a*), $(A \setminus B) \cup (A \cap B)$, onde $A \setminus B$ e $A \cap B$ são disjuntos. Portanto,

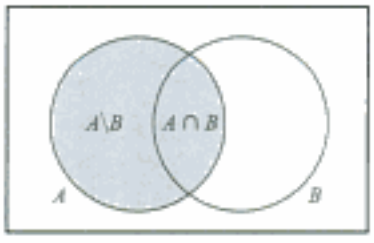
$$P(A) = P(A \setminus B) + P(A \cap B)$$

de onde segue o resultado.

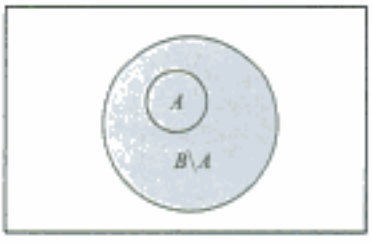
(iii) Se $A \subseteq B$, então, como indicado na Figura 7-5(*b*), $B = A \cup (B \setminus A)$, onde A e $B \setminus A$ são disjuntos. Portanto,

$$P(B) = P(A) + P(B \setminus A)$$

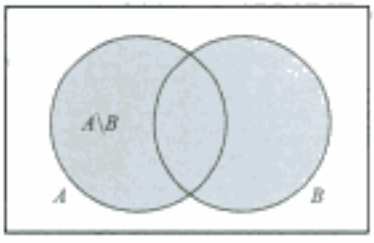
Como $P(B \setminus A) \geq 0$, temos $P(A) \leq P(B)$.



(*a*) A está sombreado.



(*b*) B está sombreado.



(*c*) $A \cup B$ está sombreado.

Fig. 7-5

7.17 Prove o Teorema 7.4 (princípio da adição): Para quaisquer eventos A e B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Como indicado na Figura 7-5 (c), $A \cup B = (A \setminus B) \cup B$, onde $A \setminus B$ e B são conjuntos disjuntos. Logo, usando o Teorema 7.3(ii)

$$\begin{aligned} P(A \cup B) &= P(A \setminus B) + P(B) = P(A) - P(A \cap B) + P(B) \\ &= P(A) + P(B) - P(A \cap B) \end{aligned}$$

Probabilidade Condicional

7.18 Três moedas confiáveis são jogadas. Ache a probabilidade p de que todos os resultados sejam cara se: (a) a primeira moeda der cara; (b) pelo menos uma das moedas der cara.

O espaço amostral tem oito elementos $S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$.

(a) Se a primeira é cara, o espaço amostral restrito é $A = \{\text{HHH, HHT, HTH, HTT}\}$. Como todas as moedas produzem cara em um dos quatro casos, $p = \frac{1}{4}$.

(b) Se uma ou mais dentre as moedas é cara, o espaço amostral restrito é

$$B = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH}\}.$$

Como todos os resultados são cara em um de sete casos, $p = \frac{1}{7}$.

7.19 Um par de dados confiáveis é jogado. Ache a probabilidade p de se obter soma maior ou igual a 10 se: (a) o primeiro dado cair com 5; (b) pelo menos um dos dados cair com 5.

(a) Se 5 aparece no primeiro dado, o espaço amostral reduzido é

$$A = \{(5,1),\ (5,2),\ (5,3),\ (5,4),\ (5,5),\ (5,6)\}$$

A soma é maior ou igual a 10 em dois dos seis resultados, (5, 5) e (5, 6). Portanto $p = \frac{2}{6} = \frac{1}{3}$.

(b) Se 5 aparece em pelo menos um dos dados, então o espaço amostral restrito tem 11 elementos.

$$B = \{(5,1),\ (5,2),\ (5,3),\ (5,4),\ (5,5),\ (5,6),\ (1,5),\ (2,5),\ (3,5),\ (4,5),\ (6,5)\}$$

A soma é maior ou igual a 10 em três dos 11 resultados: (5, 5), (5, 6) (6, 5). Portanto, $p = \frac{3}{11}$.

7.20 Em uma certa universidade, 25% dos estudantes foram reprovados em matemática, 15% em química e 10% em ambas as disciplinas. Um estudante é selecionado aleatoriamente.

(a) Se ele foi reprovado em química, qual é a probabilidade de ter sido reprovado em matemática?

(b) Se ele foi reprovado em matemática, qual é a probabilidade de ter sido reprovado em química?

(c) Qual é a probabilidade de que ele tenha sido reprovado em matemática ou química?

(d) Qual é a probabilidade de que ele não tenha sido reprovado nem em matemática nem em química?

(a) A probabilidade de que o estudante tenha sido reprovado em matemática, considerando que foi reprovado em química, é

$$P(M \mid Q) = \frac{P(M \cap Q)}{P(Q)} = \frac{0{,}10}{0{,}15} = \frac{2}{3}$$

(b) A probabilidade de que o estudante tenha sido reprovado em química, considerando que foi reprovado em matemática, é

$$P(C \mid M) = \frac{P(Q \cap M)}{P(M)} = \frac{0{,}10}{0{,}25} = \frac{2}{5}$$

(c) Pelo princípio da adição (Teorema 7.4),

$$P(M \cup Q) = P(M) + P(Q) - P(M \cap Q) = 0{,}25 + 0{,}15 - 0{,}10 = 0{,}30$$

(*d*) Estudantes que não foram reprovados nem em matemática nem em química formam o complementar do conjunto $M \cup Q$, isto é, formam o conjunto $(M \cup Q)^c$. Portanto,

$$P((M \cup Q)^c) = 1 - P(M \cup Q) = 1 - 0{,}30 = 0{,}70$$

7.21 Um par de dados confiáveis é jogado. Se os dois números que aparecem são diferentes, ache a probabilidade p de que: (*a*) a soma seja 6; (*b*) apareça um 1; (*c*) a soma seja menor ou igual a 4.

Existem 36 maneiras pelas quais um par de dados pode cair, e seis delas, (1, 1), (2, 2),..., (6, 6), têm os mesmos números. Portanto, o espaço amostral restrito consistirá em 36 – 6 = 30 elementos.

(*a*) A soma 6 pode aparecer de quatro maneiras: (1, 5), (2, 4), (4, 2), (5, 1). (Não podemos incluir (3, 3) já que os números são os mesmos.) Portanto, $p = \frac{4}{30} = \frac{2}{15}$.

(*b*) Um 1 pode aparecer de 10 maneiras: (1, 2), (1, 3)..., (1, 6) e (2, 1), (3, 1),..., (6, 1). Portanto, $p = \frac{10}{30} = \frac{1}{3}$.

(*c*) A soma menor ou igual a 4 pode ocorrer de quatro maneiras: (3, 1), (1, 3), (2, 1), (1, 2). Portanto, $p = \frac{4}{30} = \frac{2}{15}$.

7.22 Uma turma tem 12 meninos e quatro meninas. Suponha que três estudantes são aleatoriamente selecionados na turma. Ache a probabilidade p de que sejam todos meninos.

A probabilidade de que o primeiro estudante selecionado seja um menino é 12/16, já que existem 12 meninos entre os 16 estudantes. Se o primeiro estudante é um menino, então a probabilidade do segundo ser menino é 11/15, já que existem 11 meninos remanescentes entre 15 estudantes. Finalmente, se os primeiros dois estudantes selecionados forem meninos, a probabilidade de que o terceiro seja um menino é 10/14, já que existem 10 meninos restantes entre 14 estudantes. Portanto, pelo teorema da multiplicação, a probabilidade de os três serem meninos é

$$p = \frac{12}{16} \cdot \frac{11}{15} \cdot \frac{10}{14} = \frac{11}{28}$$

Outro método: Existem $C(16, 3) = 560$ maneiras de selecionar três estudantes entre 16 estudantes, e $C(12, 3) = 220$ maneiras de selecionar três meninos entre 12 meninos; logo,

$$p = \frac{220}{560} = \frac{11}{28}$$

Outro método: Se os estudantes forem selecionados um após o outro, então existem $16 \cdot 15 \cdot 14$ maneiras de selecionar três estudantes e $12 \cdot 11 \cdot 10$ maneiras de selecionar três meninos; logo,

$$p = \frac{12 \cdot 11 \cdot 10}{16 \cdot 15 \cdot 14} = \frac{11}{28}$$

7.23 Ache $P(B \mid A)$ se: (*a*) A é um subconjunto de B; (*b*) A e B são mutuamente excludentes. (Assuma $P(A) > 0$.)

(*a*) Se A é um subconjunto de B [como indicado na Figura 7-6(*a*)], então sempre que A ocorre, B precisa ocorrer; portanto, $P(B \mid A) = 1$. De outra forma, se A for um subconjunto de B, então $A \cap B = A$; portanto,

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{P(A)}{P(A)} = 1$$

(*b*) Se A e B são mutuamente excludentes, i.e., disjuntos [como representado na Figura 7-6 (*b*)], então, sempre que A ocorre, B não pode ocorrer; logo, $P(B \mid A) = 0$. Resolvendo de outro modo, se A e B são disjuntos, então $A \cap B = \varnothing$; logo,

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{P(= \varnothing)}{P(A)} = \frac{0}{P(A)} = 0$$

(*a*) $A \subseteq B$ (*b*) $A \cap B = \varnothing$

Fig. 7-6

Independência

7.24 A probabilidade de que A atinja o alvo é $\frac{1}{3}$, e a probabilidade de que B atinja o alvo é $\frac{1}{5}$. Ambos atiram no alvo. Ache a probabilidade de que: (*a*) A não atinja o alvo; (*b*) ambos atinjam o alvo; (*c*) um deles atinja o alvo; (*d*) nenhum atinja o alvo.

Sabemos que $P(A) = \frac{1}{3}$ e $P(B) = \frac{1}{5}$ (e assumimos que os eventos são independentes).

(*a*) P (não A) $= P(A^c) = 1 - P(A) = 1 - \frac{1}{3} = \frac{2}{3}$.

(*b*) Como os eventos são independentes,

$$P(A \text{ e } B) = P(A \cap B) = P(A) \cdot P(B) = \tfrac{1}{3} \cdot \tfrac{1}{5} = \tfrac{1}{15}$$

(*c*) Pelo princípio da adição (Teorema 7.4),

$$P(A \text{ ou } B) = P(A \cup B) = P(A) + P(B) - P(A \cap B) = \tfrac{1}{3} + \tfrac{1}{5} - \tfrac{1}{15} = \tfrac{7}{15}$$

(*d*) Temos

$$P(\text{nem } A \text{ nem } B) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - \tfrac{7}{15} = \tfrac{8}{15}$$

7.25 Considere os seguintes eventos em uma família com crianças:

$$A = \{\text{crianças de ambos os sexos}\}, \quad B = \{\text{no máximo um menino}\}$$

(*a*) Mostre que A e B são eventos independentes se uma família tem três crianças.

(*b*) Mostre que A e B são eventos dependentes se uma família tem apenas duas crianças.

(*a*) Temos o espaço equiprovável $S = \{bbb, bbg, bgb, bgg, gbb, gbg, ggb, ggg\}$[†]. Aqui,

$$\begin{aligned} A &= \{bbg, bgb, bgg, gbb, gbg, ggb\} && \text{e, logo,} && P(A) = \tfrac{6}{8} = \tfrac{3}{4} \\ B &= \{bgg, gbg, ggb, ggg\} && \text{e, logo,} && P(B) = \tfrac{4}{8} = \tfrac{1}{2} \\ A \cap B &= \{bgg, gbg, ggb\} && \text{e, logo,} && P(A \cap B) = \tfrac{3}{8} \end{aligned}$$

Como $P(A)P(B) = \frac{3}{4} \cdot \frac{1}{2} = \frac{3}{8} = P(A \cap B)$, A e B são independentes.

(*b*) Temos o espaço equiprovável $S = \{bb, bg, gb, gg\}$. Aqui,

$$\begin{aligned} A &= \{bg, gb\} && \text{e, logo,} && P(A) = \tfrac{1}{2} \\ B &= \{bg, gb, gg\} && \text{e, logo,} && P(B) = \tfrac{3}{4} \\ A \cap B &= \{bg, gb\} && \text{e, logo,} && P(A \cap B) = \tfrac{1}{2} \end{aligned}$$

Como $P(A)P(B) \neq P(A \cap B)$, A e B são dependentes.

[†] N. de T. Aqui, b representa menino (*boy*) e g é usado para menina (*girl*).

7.26 A caixa A contém cinco bolas de gude vermelhas e três azuis, e a caixa B contém três vermelhas e duas azuis. Uma bola de gude é aleatoriamente retirada de cada caixa.

(a) Ache a probabilidade p de que ambas as bolas sejam vermelhas.

(b) Ache a probabilidade p de que uma bola seja vermelha e a outra, azul.

(a) A probabilidade de escolher uma bola vermelha de A é $\frac{5}{8}$ e de B é $\frac{3}{5}$. Como os eventos são independentes, $p = \frac{5}{8} \cdot \frac{3}{5} = \frac{3}{8}$.

(b) A probabilidade p_1 de escolher uma bola vermelha de A e uma azul de B é $\frac{5}{8} \cdot \frac{2}{5} = \frac{1}{4}$. A probabilidade p_2 de escolher uma bola azul de A e uma bola vermelha de B é $\frac{3}{8} \cdot \frac{3}{5} = \frac{9}{40}$. Portanto, $p = p_1 + p_2 = \frac{1}{4} + \frac{9}{40} = \frac{19}{40}$.

7.27 Prove: se A e B são eventos independentes, então A^C e B^C são eventos independentes.

Sejam $P(A) = x$ e $P(B) = y$. Então, $P(A^c) = 1 - x$ e $P(B^c) = 1 - y$. Como A e B são independentes, $P(A \cap B) = P(A)P(B) = xy$. Além disso,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = x + y - xy$$

Pela lei de DeMorgan, $(A \cup B)^c = A^c \cap B^c$; logo,

$$P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - x - y + xy$$

Por outro lado,

$$P(A^c)P(B^c) = (1 - x)(1 - y) = 1 - x - y + xy$$

Logo, $P(A^c \cap B^c) = P(A^c)P(B^c)$, e, portanto, A^c e B^c são independentes.

De modo semelhante, podemos mostrar que A e B^c, bem como A^c e B, são independentes.

Tentativas Repetidas e Distribuição Binominal

7.28 Sempre que os cavalos a, b, c e d correm juntos, suas respectivas probabilidades de vitória são 0,2, 0,5, 0,1 e 0,2. Isto é, $S = \{a, b, c, d\}$, onde $P(a) = 0{,}2$, $P(b) = 0{,}5$, $P(c) = 0{,}1$ e $P(d) = 0{,}2$. Eles competem três vezes.

(a) Descreva e ache o número de elementos no espaço produto de probabilidade S_3.

(b) Ache a probabilidade de que o mesmo cavalo ganhe os três páreos.

(c) Ache a probabilidade de que a, b e c ganhem, cada um, um páreo.

(a) Por definição, $S_3 = S \times S \times S = \{(x, y, z) : x, y, z \in S\}$ e

$$P(x, y, z) = P(x)P(y)P(z)$$

Portanto, em particular, S_3 contém $4^3 = 64$ elementos.

(b) Escrevendo xyz para (x, y, z), procuramos a probabilidade do evento

$$A = \{aaa, bbb, ccc, ddd\}$$

Por definição,

$$P(aaa) = (0{,}2)^3 = 0{,}008, \qquad P(ccc) = (0{,}1)^3 = 0{,}001$$
$$P(bbb) = (0{,}5)^3 = 0{,}125, \qquad P(ddd) = (0{,}2)^3 = 0{,}008$$

Portanto, $P(A) = 0{,}0008 + 0{,}125 + 0{,}001 + 0{,}008 = 0{,}142$.

(c) Procuramos a probabilidade do evento

$$B = \{abc, acb, bac, bca, cab, cba\}$$

Todo elemento em B tem a mesma probabilidade. Portanto,

$(0{,}2)(0{,}5)(0{,}1) = 0{,}01$. Logo, $P(B) = 6(0{,}01) = 0{,}06$.

7.29 Uma moeda confiável é lançada três vezes. Ache a probabilidade de ocorrência de: (*a*) três caras; (*b*) exatamente duas caras; (*c*) exatamente uma cara; (*d*) nenhuma cara.

Suponha que H denote uma cara e T, uma coroa em qualquer um dos lances. Os três lances podem ser modelados como um espaço equiprovável onde existem oito resultados possíveis:

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

Entretanto, como o resultado em qualquer lance não depende do resultado em nenhum outro lance, as três jogadas podem ser modeladas como três tentativas independentes nas quais $P(H) = \frac{1}{2}$ e $P(T) = \frac{1}{2}$ em qualquer uma delas. Então:

(*a*) $P(\text{três caras}) = P(\text{HHH}) = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$.

(*b*) $P(\text{exatamente duas caras}) = P(\text{HHT ou HTH ou THH})$
$$= \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{3}{8}$$

(*c*) Como em (*b*), P (exatamente uma cara) = P(exatamente uma coroa) = $\frac{3}{8}$.

(*d*) Como em (*a*), P (nenhuma cara) = P (três coroas) = $\frac{1}{8}$.

7.30 A probabilidade de que João atinja o alvo é $p = \frac{1}{4}$. Ele atira $n = 6$ vezes. Ache a probabilidade de que ele atinja o alvo: (*a*) exatamente duas vezes; (*b*) mais de quatro vezes; (*c*) pelo menos uma vez.

Este é um experimento binomial com $n = 6$, $p = \frac{1}{4}$, e $q = 1 - p = \frac{3}{4}$; isto é, $B(6, \frac{1}{4})$. Por conseguinte, usamos o Teorema 7.7.

(*a*) $P(2) = \binom{6}{2}(\frac{1}{4})^2(\frac{3}{4})^4 = 15(3^4)/(4^6) = \frac{1215}{4.096} \approx 0{,}297.$

(*b*) $P(5) + P(6) = \binom{6}{5}(\frac{1}{4})^5(\frac{3}{4})^1 + (\frac{1}{4})^6 = \frac{18^6}{4} + \frac{1^6}{4} = \frac{19^6}{4} = \frac{19}{4.096} \approx 0{,}0046.$

(*c*) $P(0) = (\frac{3}{4})^6 = \frac{729}{4.096}$; logo, $P(X > 0) = 1 - \frac{729}{4.096} = \frac{3.367}{4.096} \approx 0{,}82.$

7.31 Suponha que 20% dos itens produzidos em uma fábrica sejam defeituosos. Suponha que quatro itens sejam escolhidos aleatoriamente. Ache a probabilidade de que: (*a*) dois sejam defeituosos; (*b*) três sejam defeituosos; (*c*) nenhum seja defeituoso.

Este é um experimento binomial com $n = 4$, $p = 0{,}2$ e $q = 1 - p = 0{,}8$; isto é, $B(4, 0{,}2)$. Logo, usando o Teorema 7.7.

(*a*) $P(2) = \binom{4}{2}(0{,}2)^2(0{,}8)^2 = 0{,}1536.$

(*b*) $P(3) = \binom{4}{3}(0{,}2)^3(0{,}8)^1 = 0{,}0256.$

(*c*) $P(0) = (0{,}8)^4 = 0{,}4095.$

7.32 O time A tem a probabilidade $\frac{2}{3}$ de ganhar sempre que joga. Suponha que A jogue quatro partidas. Ache a probabilidade p de que A ganhe mais da metade destas partidas.

Aqui, $n = 4$, $p = \frac{2}{3}$ e $q = 1 - p = \frac{1}{3}$. A ganha mais da metade das partidas se ganhar três das quatro partidas.

$$p = P(3) + P(4) = \binom{4}{3}\left(\frac{2}{3}\right)^3\left(\frac{1}{3}\right)^1 + \binom{4}{4}\left(\frac{2}{3}\right)^4 = \frac{32}{81} + \frac{16}{81} = \frac{16}{27} = 0{,}59$$

7.33 Uma família tem seis crianças. Ache a probabilidade p de que elas sejam: (*a*) três meninos e três meninas; (*b*) menos meninos do que meninas. Assuma que a probabilidade de qualquer criança ser menino é $\frac{1}{2}$.

Aqui, $n = 6$ e $p = q = \frac{1}{2}$.

(*a*) $p = P(3 \text{ meninos}) = \binom{6}{3}\left(\frac{1}{2}\right)^3\left(\frac{1}{2}\right)^2 = \frac{20}{64} = \frac{5}{16}$.

(*b*) Existem menos meninos do que meninas se existirem zero, um ou dois meninos. Portanto,

$$p = P(0 \text{ menino}) + P(1 \text{ menino}) + P(2 \text{ meninos}) = \left(\frac{1}{2}\right)^6 + \binom{6}{1}\left(\frac{1}{2}\right)^5 + \binom{6}{2}\left(\frac{1}{2}\right)^2\left(\frac{1}{2}\right)^4 = \frac{11}{32} = 0{,}34$$

7.34 Um certo tipo de míssil atinge seu alvo com probabilidade $p = 0{,}3$. Ache o número de mísseis que devem ser lançados para que exista uma probabilidade de pelo menos 80% de o alvo ser atingido.

A probabilidade de o míssil não atingir o alvo é $q = 1 - p = 0{,}7$. Portanto, a probabilidade de que n mísseis não atingem o alvo é $(0{,}7)^n$. Portanto, procuramos o menor n para o qual

$$1 - (0{,}7)^n > 0{,}8 \qquad \text{ou, de modo equivalente,} \qquad (0{,}7)^n < 0{,}2$$

Compute:

$$(0{,}7)^1 = 0{,}7, \qquad (0{,}7)^2 = 0{,}49, \qquad (0{,}7)^3 = 0{,}343, \qquad (0{,}7)^4 = 0{,}2401, \qquad (0{,}7)^5 = 0{,}16807$$

Portanto, pelo menos cinco mísseis devem ser lançados.

7.35 Quantos dados devem ser lançados de tal maneira que exista uma chance maior do que metade de se obter um 6?

A probabilidade de não se obter um 6 em n dados é $\left(\frac{5}{6}\right)^n$. Portanto, procuramos o menor n para o qual $\left(\frac{5}{6}\right)^n$ seja menor do que $\frac{1}{2}$. Calcule como a seguir:

$$\left(\frac{5}{6}\right)^1 = \frac{5}{6}, \qquad \left(\frac{5}{6}\right)^2 = \frac{25}{36}, \qquad \left(\frac{5}{6}\right)^3 = \frac{125}{216}, \qquad \text{mas} \qquad \left(\frac{5}{6}\right)^4 = \frac{625}{1296} < \frac{1}{2}$$

Logo, quatro dados precisam ser jogados.

7.36 Um certo time de futebol vence (V) com probabilidade 0,6, perde (P) com probabilidade 0,3 e empata (E) com probabilidade 0,1. O time joga três vezes no final de semana. (*a*) Determine os elementos do evento A em que o time ganha pelo menos duas vezes e não perde e ache $P(A)$. (*b*) Determine os elementos do evento B em que o time ganha, perde e empata em alguma ordem e ache $P(B)$.

(*a*) A consiste nas triplas ordenadas com pelo menos dois Vs e nenhum P. Logo,

$$A = \{\text{VVV, VVE, VEV, EVV}\}$$

Além disso,

$$\begin{aligned} P(A) &= P(\text{VVV}) + P(\text{VVE}) + P(\text{VEV}) + P(\text{EVV}) \\ &= (0{,}6)(0{,}6)(0{,}6) + (0{,}6)(0{,}6)(0{,}1) + (0{,}6)(0{,}1)(0{,}6) + (0{,}1)(0{,}6)(0{,}6) \\ &= 0{,}216 + 0{,}036 + 0{,}036 + 0{,}036 = 0{,}324 \end{aligned}$$

(*b*) Aqui, $B = \{\text{VPE, VEP, PVE, PEV, EVP, EPV}\}$. Todo elemento em B tem a probabilidade (0,6) (0,3) (0,1) = 0,018; logo, $P(B) = 6\,(0{,}018) = 0{,}108$.

7.37 Um homem atira em um alvo $n = 6$ vezes e o atinge $k = 2$ vezes. (*a*) Liste as diferentes maneiras pelas quais isso pode acontecer.

(*a*) Liste todas as seqüências com dois Ss (sucessos) e quatro Fs (fracassos):

SSFFFF, SFSFFF, SFFSFF, SFFFSF, SFFFFS, FSSFFF, FSFSFF, FSFFSF,
FSFFFS, FFSSFF, FFSFSF, FFSFFS, FFFSSF, FFFSFS, FFFFSS

(*b*) Existem 15 maneiras diferentes, como indicado na lista. Observe que isto é igual a $\binom{6}{2}$, já que estamos distribuindo $k = 2$ letras S entre as $n = 6$ posições da seqüência.

7.38 Prove o Teorema 7.7: a probabilidade de exatamente k sucessos em um experimento binomial $B(n, p)$ é dada por

$$P(k) = P(k \text{ sucessos}) = \binom{n}{k} p^k q^{n-k}$$

A probabilidade de um ou mais sucessos é $1 - q^n$.

O espaço amostral de n tentativas repetidas consiste em todas as n-uplas (i.e., seqüências com n elementos) cujos componentes são S (sucesso) ou F (fracasso). Seja A o evento ocorrência de exatamente k sucessos. Então, A consiste em todas as n-uplas nas quais k componentes são S e $n - k$ componentes são F. O número de tais n-uplas no evento A é igual ao número de maneiras que k letras S podem ser distribuídas entre os n componentes de uma n-upla; portanto, A consiste em $C(n, k) = \binom{n}{k}$ amostras. A probabilidade de cada ponto em A é $p^k q^{n-k}$; logo,

$$P(A) = \binom{n}{k} p^k q^{n-k}$$

Em particular, a probabilidade de nenhum sucesso é

$$P(0) = \binom{n}{0} p^0 q^n = q^n$$

Então, a probabilidade de um ou mais sucessos é $1 - q^n$.

Variáveis Aleatórias e Expectâncias

7.39 Um jogador lança duas moedas confiáveis. Ele ganha \$ 2 se duas caras ocorrerem, e \$ 1 se uma cara ocorrer. Por outro lado, ele perde \$ 3 se nenhuma cara ocorrer. Ache o valor esperado E do jogo. O jogo é honesto? (O jogo é honesto, favorável ou desfavorável ao jogador de acordo com $E = 0$, $E > 0$ ou $E < 0$.)

O espaço amostral é $S = \{\text{HH, HT, TH, TT}\}$ e cada amostra tem probabilidade $\frac{1}{4}$. Para o ganho do jogador, temos

$$X(\text{HH}) = \$\,2, \qquad X(\text{HT}) = X(\text{TH}) = \$\,1, \qquad X(\text{TT}) = \$\,-3$$

e, portanto, a distribuição de X é

x_i	2	1	−3
p_i	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{1}{4}$

e

$$E = E(X) = 2\left(\tfrac{1}{4}\right) + 1\left(\tfrac{2}{4}\right) - 3\left(\tfrac{1}{4}\right) = \$\,0{,}25$$

Como $E(X) > 0$, o jogo é favorável ao jogador.

7.40 Dois números de 1 a 3 são escolhidos aleatoriamente, e são permitidas repetições. Seja X a soma dos números. (*a*) Ache a distribuição de X. (*b*) Ache a expectância $E(X)$.

(*a*) Existem nove pares equiprováveis compondo o espaço amostral S. X assume os valores 2, 3, 4, 5 e 6 com as seguintes probabilidades:

$$P(2) = P(1,1) = \tfrac{1}{9}, \qquad P(3) = P(\{(1,2),(2,1)\}) = \tfrac{2}{9}$$
$$P(4) = P(\{(1,3),(2,2),(3,1)\}) = \tfrac{3}{9}$$
$$P(5) = P(\{(2,3),(3,2)\}) = \tfrac{2}{9}, \qquad P(6) = P(3,3) = \tfrac{1}{9}$$

Portanto, a distribuição é

x_i	2	3	4	5	6
$P(x_i)$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{3}{9}$	$\frac{2}{9}$	$\frac{1}{9}$

(*b*) O valor esperado $E(X)$ é obtido multiplicando cada valor de x pela sua probabilidade e efetuando a soma. Portanto,

$$E(X) = 2\left(\tfrac{1}{9}\right) + 3\left(\tfrac{2}{9}\right) + 4\left(\tfrac{3}{9}\right) + 5\left(\tfrac{2}{9}\right) + 6\left(\tfrac{1}{9}\right) = \tfrac{36}{9} = 4$$

7.41 Uma moeda tem seu peso distribuído de tal maneira que $P(H) = \frac{3}{4}$ e $P(T) = \frac{1}{4}$. A moeda é jogada três vezes. Seja X o número de ocorrência de caras. (*a*) Ache a distribuição de X. (*b*) Ache a expectância $E(X)$.

(*a*) O espaço amostral é:

$$S = \{\text{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT}\}$$

X assume os valores 0, 1, 2 e 3 com as seguintes probabilidades:

$$P(0) = P(\text{TTT}) = \tfrac{1}{4}\cdot\tfrac{1}{4}\cdot\tfrac{1}{4} = \tfrac{1}{64}$$
$$P(1) = P(\text{HTT, THT, TTH}) = \tfrac{3}{4}\cdot\tfrac{1}{4}\cdot\tfrac{1}{4} + \tfrac{1}{4}\cdot\tfrac{3}{4}\cdot\tfrac{1}{4} + \tfrac{1}{4}\cdot\tfrac{1}{4}\cdot\tfrac{3}{4} = \tfrac{9}{64}$$
$$P(2) = P(\text{HHT, HTH, THH}) = \tfrac{3}{4}\cdot\tfrac{3}{4}\cdot\tfrac{1}{4} + \tfrac{3}{4}\cdot\tfrac{1}{4}\cdot\tfrac{3}{4} + \tfrac{1}{4}\cdot\tfrac{3}{4}\cdot\tfrac{3}{4} = \tfrac{27}{64}$$
$$P(3) = P(\text{HHH}) = \tfrac{3}{4}\cdot\tfrac{3}{4}\cdot\tfrac{3}{4} = \tfrac{27}{64}$$

Portanto, a distribuição é a seguinte:

x_i	0	1	2	3
$P(x_i)$	$\frac{1}{64}$	$\frac{9}{64}$	$\frac{27}{64}$	$\frac{27}{64}$

(*b*) O valor esperado $E(X)$ é obtido multiplicando cada valor de x pela sua probabilidade e efetuando a soma. Portanto,

$$E(X) = 0\left(\tfrac{1}{64}\right) + 1\left(\tfrac{9}{64}\right) + 2\left(\tfrac{27}{64}\right) + 3\left(\tfrac{27}{64}\right) = \tfrac{144}{64} = 2{,}25$$

7.42 Você ganhou uma disputa. Seu prêmio é selecionar um dentre três envelopes e ficar com que houver nele. Dois envelopes contêm um cheque de \$ 30, mas o terceiro envelope contém um cheque de \$ 3.000. Qual é a expectância E dos seus ganhos (como distribuição de probabilidades)?

Suponha que X denote os seus ganhos. Então, $X = 30$ ou 3.000, e $P(30) = \frac{2}{3}$ e $P(3.000) = \frac{1}{3}$. Logo,

$$E = E(X) = 30\cdot\tfrac{2}{3} + 3.000\cdot\tfrac{1}{3} = 20 + 1.000 = 1.020$$

7.43 Uma moeda confiável é jogada até que uma cara ou cinco coroas apareçam. Ache o número esperado E de lançamentos da moeda.

Os resultados possíveis são

$$\text{H,} \quad \text{TH,} \quad \text{TTH,} \quad \text{TTTH,} \quad \text{TTTTH,} \quad \text{TTTTT}$$

com suas respectivas probabilidades (tentativas independentes)

$$\tfrac{1}{2}, \quad \left(\tfrac{1}{2}\right)^2 = \tfrac{1}{4}, \quad \left(\tfrac{1}{2}\right)^3 = \tfrac{1}{8}, \quad \left(\tfrac{1}{2}\right)^4 = \tfrac{1}{16}, \quad \left(\tfrac{1}{2}\right)^5 = \tfrac{1}{32}, \quad \left(\tfrac{1}{2}\right)^5 = \tfrac{1}{32}$$

A variável aleatória X que interessa é o número de lançamentos em cada resultado. Logo,

$$X(\text{H}) = 1, \quad X(\text{TTH}) = 3, \quad X(\text{TTTTH}) = 5$$
$$X(\text{TH}) = 2, \quad X(\text{TTTH}) = 4, \quad X(\text{TTTTT}) = 5$$

e esses valores de X tem probabilidades

$$P(1) = P(\text{H}) = \tfrac{1}{2}, \quad P(3) = P(\text{TTH}) = \tfrac{1}{8}, \quad P(5) = P(\text{TTTTH}) + P(\text{TTTTT}) = \tfrac{1}{32} + \tfrac{1}{32} = \tfrac{1}{16}$$
$$P(2) = P(\text{TH}) = \tfrac{1}{4}, \quad P(4) = P(\text{TTTH}) = \tfrac{1}{16},$$

Conseqüentemente,

$$E = E(X) = 1\cdot\tfrac{1}{2} + 2\cdot\tfrac{1}{4} + 3\cdot\tfrac{1}{8} + 4\cdot\tfrac{1}{16} + 5\cdot\tfrac{1}{16} \approx 1{,}9$$

7.44 Um *array* linear EMPREGADO tem n elementos. Suponha que NOME apareça aleatoriamente no *array*, e que exista uma busca linear para achar a posição K de NOME, isto é, para determinar K tal que EMPREGADO[K] = NOME. Seja $f(n)$ o número de comparações na busca linear.

(*a*) Ache o valor esperado de $f(n)$.

(*b*) Ache o valor máximo (pior caso) de $f(n)$.

(*a*) Seja X o número de comparações. Como NOME pode aparecer em qualquer posição no *array* com a mesma probabilidade de $1/n$, temos $X = 1, 2, 3\ldots, n$, cada um com probabilidade $1/n$. Logo,

$$f(n) = E(X) = 1\cdot\frac{1}{n} + 2\cdot\frac{1}{n} + 3\cdot\frac{1}{n} + \cdots + n\cdot\frac{1}{n}$$
$$= (1 + 2 + \cdots + n)\cdot\frac{1}{n} = \frac{n(n+1)}{2}\cdot\frac{1}{n} = \frac{n+1}{2}$$

(*b*) Se NOME aparecer no final do *array*, então $f(n) = n$

Média, Variância e Desvio-Padrão

7.45 Ache a média $\mu = E(X)$, a variância $\sigma^2 = \mathrm{Var}\,(X)$ e o desvio-padrão $\sigma = \sigma_X$ de cada distribuição:

(*a*)

x_i	2	3	11
p_i	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{6}$

(*b*)

x_i	1	3	4	5
p_i	0,4	0,1	0,2	0,3

Use as fórmulas,

$\mu = E(X) = x_1p_1 + x_2p_2 + \cdots + x_mp_m = \Sigma x_ip_i$, $\quad \sigma^2 = \mathrm{Var}\,(X) = E(X^2) - \mu^2$

$E(X^2) = x_1^2p_1 + x_2^2p_2 + \cdots + x_m^2p_m = \Sigma x_i^2p_i$, $\quad \sigma = \sigma_X = \sqrt{\mathrm{Var}\,(X)}$

$\sigma = \sigma_X = \sqrt{\mathrm{Var}\,(X)}$

(*a*) $\mu = \Sigma x_ip_i = 2\left(\frac{1}{3}\right) + 3\left(\frac{1}{2}\right) + 11\left(\frac{1}{6}\right) = 4.$

$E(X^2) = \Sigma x_i^2p_i = 2^2\left(\frac{1}{3}\right) + 3^2\left(\frac{1}{2}\right) + 11^2\left(\frac{1}{6}\right) = 26.$

$\sigma^2 = \mathrm{Var}\,(X) = E(X^2) - \mu^2 = 26 - 4^2 = 10.$

$\sigma = \sqrt{\mathrm{Var}\,(X)} = \sqrt{10} = 3{,}2.$

(*b*) $\mu = \Sigma x_ip_i = 1(0{,}4) + 3(0{,}1) + 4(0{,}2) + 5(0{,}3) = 3.$

$E(X^2) = \Sigma x_i^2p_i = 1(0{,}4) + 9(0{,}1) + 16(0{,}2) + 25(0{,}3) = 12.$

$\sigma^2 = \mathrm{Var}\,(X) = E(X^2) - \mu^2 = 12 - 9 = 3.$

$\sigma = \sqrt{\mathrm{Var}\,(X)} = \sqrt{3} = 1{,}7.$

7.46 Cinco cartas são numeradas de 1 a 5. Duas cartas são retiradas aleatoriamente. Seja X a soma dos números retirados. Ache (*a*) a distribuição de X e (*b*) a média μ, a variância $\sigma^2 = \mathrm{Var}\,(X)$ e o desvio-padrão $\sigma = \sigma_X$ de X.

(*a*) Existem $C(5, 2) = 10$ maneiras de retirar duas cartas aleatoriamente. As 10 amostras equiprováveis, com seu valores de X correspondentes, são mostrados abaixo

$$\{1,2\} \to 3 \quad \{1,3\} \to 4 \quad \{1,4\} \to 5 \quad \{1,5\} \to 6 \quad \{2,3\} \to 5$$
$$\{2,4\} \to 6 \quad \{2,5\} \to 7 \quad \{3,4\} \to 7 \quad \{3,5\} \to 8 \quad \{4,5\} \to 9$$

Observe que os valores de X são os sete números 3, 4, 5, 6, 7, 8 e 9; entre eles, 3, 4, 8 e 9 são, cada um, assumidos em um ponto do espaço amostral, enquanto 5, 6 e 7 são assumidos, cada um, em dois pontos. Portanto, a distribuição de X é

x_i	3	4	5	6	7	8	9
p_i	0,1	0,1	0,2	0,2	0,2	0,1	0,1

(*b*) $\mu = E(X) = \Sigma x_i p_i = 3(0,1) + 4(0,1) + 5(0,2) + 6(0,2) + 7(0,2) + 8(0,1) + 9(0,1) = 6.$
$E(X^2) - \Sigma x_i^2 p_i = 9(0,1) + 16(0,1) + 25(0,2) + 36(0,2) + 49(0,2) + 64(0,1) + 81(0,1) = 39.$
$\text{Var}(X) = E(X^2) - \mu^2 = 39 - 6^2 = 3.$
$\sigma = \sqrt{\text{Var}(X)} = \sqrt{3} \approx 1,7.$

7.47 Um par de dados confiáveis é lançado. Seja X o máximo dos dois números que aparecem. Ache (*a*) a distribuição de X e (*b*) a média μ, a variância $\sigma^2 = \text{Var}(X)$ e o desvio-padrão $\sigma = \sigma_X$ de X.

(*a*) O espaço amostral S é o espaço equiprovável consistindo nos 36 pares de inteiros (a, b) onde a e b variam de 1 a 6; isto é

$$S = \{(1, 1), (1, 2), \ldots, (6, 6)\}$$

(Veja o Problema 7.3.) Como X associa a cada par em S o maior dos dois inteiros, os valores de X são os inteiros de 1 a 6. Observe:

(i) Apenas um par, (1,1), tem máximo igual a 1; logo, $P(1) = \frac{1}{36}$.

(ii) Três pares, (1, 2) (2, 2) e (2, 1), têm um máximo igual a 2; logo, $P(2) = \frac{3}{36}$.

(iii) Cinco pares, (1, 3), (2, 3), (3, 3), (3, 2) e (3, 1), têm um máximo igual a 3; logo, $P(3) = \frac{5}{36}$.

De modo semelhante, $P(4) = \frac{7}{36}$, $P(5) = \frac{9}{36}$, $P(6) = \frac{11}{36}$.

Portanto, a distribuição de X é a seguinte:

x_i	1	2	3	4	5	6
p_i	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{5}{36}$	$\frac{7}{36}$	$\frac{9}{36}$	$\frac{11}{36}$

(*b*) Achamos a expectância (média) de X multiplicando cada x_i pela sua probabilidade p_i e, então, somando:

$$\mu = E(X) = 1 \cdot \tfrac{1}{36} + 2 \cdot \tfrac{3}{36} + 3 \cdot \tfrac{5}{36} + 4 \cdot \tfrac{7}{36} + 5 \cdot \tfrac{9}{36} + 6 \cdot \tfrac{11}{36} = \tfrac{161}{36} \approx 4,5$$

Achamos $E(X^2)$ multiplicando x_i^2 por p_i e então somando:

$$E(X^2) = 1 \cdot \tfrac{1}{36} + 4 \cdot \tfrac{3}{36} + 9 \cdot \tfrac{5}{36} + 16 \cdot \tfrac{7}{36} + 25 \cdot \tfrac{9}{36} + 36 \cdot \tfrac{11}{36} = \tfrac{791}{36} \approx 22,0$$

Então,

$$\text{Var}(X) = E(X^2) - \mu^2 = 22,0 - (4,5)^2 = 1,75 \qquad \text{e} \qquad \sigma_X = \sqrt{1,75} \approx 1,3$$

7.48 Um dado confiável é jogado. Seja X o dobro do número que aparece, e seja Y igual a 1 ou 3, dependendo de o número ser ímpar ou par. Ache a distribuição e a expectância (*a*) de X; (*b*) de Y.

O espaço amostral é $S = \{1, 2, 3, 4, 5, 6\}$, onde cada ponto tem probabilidade $\frac{1}{6}$.

(*a*) As imagens dos pontos no espaço amostral são:

$$X(1) = 2, \qquad X(2) = 4, \qquad X(3) = 6, \qquad X(4) = 8, \qquad X(5) = 10, \qquad X(6) = 12$$

Como as imagens são distintas, a distribuição é

x_i	2	4	6	8	10	12
$P(x_i)$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

Logo,

$$E(X) = \sum x_i P(x_i) = \tfrac{2}{6} + \tfrac{4}{6} + \tfrac{6}{6} + \tfrac{8}{6} + \tfrac{10}{6} + \tfrac{12}{6} = 7$$

(*b*) As imagens dos pontos no espaço amostral são:

$$Y(1) = 1, \qquad Y(2) = 3, \qquad Y(3) = 1, \qquad Y(4) = 3, \qquad Y(5) = 1, \qquad Y(6) = 3$$

Cada um dos dois valores de Y, 1 e 3, é assumido em três amostras. Portanto, temos a distribuição

y_i	1	3
$P(y_i)$	$\frac{3}{6}$	$\frac{3}{6}$

Portanto,

$$E(Y) = \sum y_i P(y_i) = \tfrac{3}{6} + \tfrac{9}{6} = 2$$

7.49 Sejam X e Y as variáveis aleatórias definidas no espaço amostral S. Então, $Z = X + Y$ e $W = XY$ também são variáveis aleatórias em S definidas por

$$Z(s) = (X + Y)(s) = X(s) + Y(s) \qquad \text{e} \qquad W(s) = (XY)(s) = X(s)Y(s)$$

Sejam X e Y as variáveis aleatórias definidas no Problema 7.48.

(*a*) Ache a distribuição e a expectância de $Z = X + Y$.
Verifique que $E(X + Y) = E(X) + E(Y)$.

(*b*) Ache a distribuição e a expectância de $W = XY$.

O espaço amostral ainda é $S = \{1, 2, 3, 4, 5, 6\}$, e cada amostra ainda tem a probabilidade $\frac{1}{6}$.

(*a*) Usando $(X + Y)(s) = X(s) + Y(s)$ e os valores de X e Y do Problema 7.48, obtemos:

$$(X + Y)(1) = 2 + 1 = 3, \qquad (X + Y)(3) = 6 + 1 = 7, \qquad (X + Y)(5) = 10 + 1 = 11$$
$$(X + Y)(2) = 4 + 3 = 7, \qquad (X + Y)(4) = 8 + 3 = 11, \qquad (X + Y)(6) = 12 + 3 = 15$$

O conjunto imagem é $\{3, 7, 11, 5\}$. Cada um dos valores 3 e 15 é assumido em uma amostra e tem, portanto, probabilidade $\frac{1}{6}$; cada um dos valores 7 e 11 é assumido em duas amostras e tem, portanto, probabilidade $\frac{2}{6}$. Logo, a distribuição de $Z = X + Y$ é:

z_i	3	7	11	15
$P(z_i)$	1/6	2/6	2/6	1/6

Portanto,

$$E(X + Y) = E(Z) = \sum z_i P(z_i) = \tfrac{3}{6} + \tfrac{14}{6} + \tfrac{22}{6} + \tfrac{15}{6} = 9$$

Além disso,

$$E(X + Y) = 9 = 7 + 2 = E(X) + E(Y)$$

(*b*) Usando $XY(s) = X(s)Y(s)$, obtemos:

$$(XY)(1) = 2(1) = 2, \qquad (XY)(3) = 6(1) = 6, \qquad (XY)(5) = 10(1) = 10$$
$$(XY)(2) = 4(3) = 12, \qquad (XY)(4) = 8(3) = 24, \qquad (XY)(6) = 12(3) = 36$$

Cada um dos valores de XY é assumido em exatamente uma amostra; portanto, a distribuição de $W = XY$ é

w_i	2	6	10	12	24	36
$P(w_i)$	1/6	1/6	1/6	1/6	1/6	1/6

Portanto,

$$E(XY) = E(W) = \sum w_i P(w_i) = \tfrac{2}{6} + \tfrac{6}{6} + \tfrac{10}{6} + \tfrac{12}{6} + \tfrac{24}{6} + \tfrac{36}{6} = 15$$

[Note que $E(XY) = 15 \neq (7)(2) = E(X)E(Y)$.]

7.50 A probabilidade de que um homem atinja o alvo é $p = 0{,}1$. Ele atira $n = 100$ vezes. Ache o número esperado μ de vezes que ele atinge o alvo e o desvio-padrão σ.

Este é um experimento binomial $B(n, p)$ onde $n = 100$, $p = 0{,}1$ e $q = 1 - p = 0{,}9$. Conseqüentemente, aplicamos o Tecrema 7.9 para obter

$$\mu = np = 100(0{,}1) = 10 \qquad \text{e} \qquad \sigma = \sqrt{npq} = \sqrt{100(0{,}1)(0{,}9)} = 3$$

7.51 Um estudante faz um teste de múltipla escolha de 18 questões com quatro opções por questão. Suponha que uma das opções seja obviamente incorreta, e que o estudante tente adivinhar entre uma das opções restantes. Ache o número esperado de respostas corretas $E(X)$ e o desvio-padrão σ.

Este é um experimento binomial $B(n, p)$ onde $n = 18$, $p = \frac{1}{3}$ e $q = 1 - p = \frac{2}{3}$. Portanto,

$$E(X) = np = 18 \cdot \frac{1}{3} = 6 \qquad \text{e} \qquad \sigma = \sqrt{npq} = \sqrt{18 \cdot \frac{1}{3} \cdot \frac{2}{3}} = 2$$

7.52 Pode-se mostrar que a função expectância $E(X)$ no espaço das variáveis aleatórias em um espaço amostral S é *linear*, isto é,

$$E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$$

Use esta propriedade para mostrar $\mu = np$ para um experimento binomial $B(n, p)$.

No espaço amostral de n tentativas de Bernoulli, seja X_i (para $i = 1, 2, \ldots, n$) a variável aleatória que tem valor 1 ou 0, dependendo de a i-ésima tentativa ser um sucesso ou um fracasso. Então, cada X_i tem a distribuição

x	0	1
$P(x)$	q	p

Portanto, $E(X_i) = 0(q) + 1(p) = p$. O número total de sucessos em n tentativas é

$$X = X_1 + X_2 + \cdots + X_n$$

Usando a linearidade de E, temos

$$\begin{aligned} E(X) &= E(X_1 + X_2 + \cdots + X_n) \\ &= E(X_1) + E(X_2) + \cdots + E(X_n) \\ &= p + p + \cdots + p = np \end{aligned}$$

Problemas Complementares

7.53 Sejam A e B eventos. Reescreva cada um dos seguintes eventos usando a notação de conjuntos: (*a*) A ou não B ocorre; (*b*) apenas A ocorre.

7.54 Sejam A, B e C eventos. Reescreva cada um dos seguintes eventos usando a notação de conjuntos: (*a*) A e B, mas não C ocorre; (*b*) A ou C, mas não B ocorre; (*c*) nenhum dos eventos ocorre; (*d*) pelo menos um dos eventos ocorre.

7.55 Um dado e duas moedas são jogados.

(*a*) Descreva um espaço amostral conveniente S e ache $n(S)$.

(*b*) Expresse explicitamente os seguintes eventos:

$$A = \{\text{duas caras e um número par}\}, \quad B = \{2 \text{ ocorre}\}$$
$$C = \{\text{exatamente uma cara e um número ímpar}\}$$

(*c*) Expresse explicitamente os eventos (i) A e B; (ii) apenas B; (iii) B e C.

Espaços Finitos Equiprováveis

7.56 Determine a probabilidade de cada um dos eventos:

(*a*) Um número ímpar aparece no lançamento de um dado confiável.

(*b*) Uma ou mais caras aparecem no lançamento de quatro moedas confiáveis.

(*c*) Um ou ambos os números excedem a 4 no lançamento de dois dados confiáveis.

7.57 Um estudante é aleatoriamente escolhido para representar um grupo que contém cinco estudantes de primeira série, oito de segunda série, três de terceira e dois de quarta série. Ache a probabilidade de que o estudante esteja (*a*) na primeira série; (*b*) na terceira série; (*c*) na terceira ou na quarta série.

7.58 Uma carta é selecionada aleatoriamente de 50 cartas numeradas de 1 a 50. Ache a probabilidade de que o número da carta seja: (*a*) maior do que 10; (*b*) divisível por 5; (*c*) maior do que 10 e divisível por 5; (*d*) maior do que 10 ou divisível por 5.

7.59 Dentre 10 garotas de uma turma, três têm olhos azuis. Duas delas são escolhidas aleatoriamente. Ache a probabilidade de que (*a*) ambas tenham olhos azuis; (*b*) nenhuma tenha olhos azuis; (*c*) pelo menos uma tenha olhos azuis; (*d*) exatamente uma tenha olhos azuis.

7.60 Dez estudantes, A, B,..., estão em uma turma. Um comitê é aleatoriamente escolhido para representar a classe. Ache a probabilidade de que (*a*) A pertença ao comitê; (*b*) B pertença ao comitê; (*c*) A e B pertençam ao comitê; (*d*) A ou B pertençam ao comitê.

7.61 Três parafusos e três porcas estão em uma caixa. Duas peças são aleatoriamente escolhidas. Ache a probabilidade de que uma seja um parafuso e a outra, uma porca.

7.62 Uma caixa contém duas meias brancas, duas azuis e duas vermelhas. Duas meias são aleatoriamente retiradas. Ache a probabilidade de que elas combinem (sejam da mesma cor).

7.63 Dentre 120 estudantes, 60 estão estudando francês, 50 estão estudando espanhol e 20 estudam ambas as línguas. Um estudante é escolhido aleatoriamente. Ache a probabilidade de que ele esteja estudando: (*a*) francês ou espanhol; (*b*) nem francês nem espanhol; (*c*) apenas francês; (*d*) exatamente um dos dois idiomas.

7.64 Três meninos e três meninas sentam aleatoriamente em fila. Ache a probabilidade de que: (*a*) as três meninas sentem juntas; (*b*) os meninos e as meninas sentem em lugares alternados.

Espaços de Probabilidade Finitos

7.65 Munido de quais das seguinte funções, $S = \{a_1, a_2, a_3\}$ é um espaço de probabilidade?

(*a*) $P(a_1) = \frac{1}{4}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$.
(*b*) $P(a_1) = \frac{2}{3}, P(a_2) = -\frac{1}{3}, P(a_3) = \frac{2}{3}$.
(*c*) $P(a_1) = \frac{1}{6}, P(a_2) = \frac{1}{3}, P(a_3) = \frac{1}{2}$.
(*d*) $P(a_1) = 0, P(a_2) = \frac{1}{3}, P(a_3) = \frac{2}{3}$.

7.66 Uma moeda tem sua massa distribuída de tal maneira que é três vezes mais provável aparecer cara do que coroa. Ache $P(H)$ e $P(T)$.

7.67 Três estudantes, A, B e C, estão participando de uma competição de natação. A e C têm a mesma probabilidade de vitória, e cada um deles tem o dobro da probabilidade de C de ganhar. Ache a probabilidade de que: (*a*) B ganhe; (*b*) C ganhe; (*c*) B ou C ganhe.

7.68 Considere a seguinte distribuição de probabilidade:

Resultado	1	2	3	4	5	6
Probabilidade	0,1	0,4	0,1	0,1	0,2	0,1

Ache as seguintes probabilidades, onde: $A = \{\text{número par}\}$, $B = \{2, 3, 4, 5\}$, $C = \{1, 2\}$.

(*a*) $P(A)$, $P(B)$, $P(C)$; (*b*) $P(A \cap B)$, $P(A \cup C)$, $P(B \cap C)$.

7.69 Suponha que A e B sejam eventos com $P(A) = 0{,}7$, $P(B) = 0{,}5$ e $P(A \cap B) = 0{,}4$. Ache a probabilidade de que: (*a*) A não ocorra; (*b*) A ou B ocorra; (*c*) nem A nem B ocorram.

7.70 Suponha que A e B sejam eventos com $P(A) = 0{,}6$, $P(B^C) = 0{,}3$ e $P(A \cup B) = 0{,}8$. Ache: (*a*) $P(A \cap B)$; (*b*) $P(A \cap B^c)$; (*c*) $P(A^c \cap B^c)$; (*d*) $P(A^c \cup B^c)$.

Probabilidade Condicional e Independência

7.71 Um dado confiável é lançado. Considere os eventos $A = \{2, 4, 6\}$, $B = \{1, 2\}$, $C = \{1, 2, 3, 4\}$. Ache:

(*a*) $P(A \text{ e } B)$ e $P(A \text{ ou } C)$, (*b*) $P(A \mid B)$ e $P(B \mid A)$,

(*c*) $P(A \mid C)$ e $P(C \mid A)$, (*d*) $P(B \mid C)$ e $P(C \mid B)$,

(*e*) A e B são independentes? A e C? B e C?

7.72 Um par de dados confiável é jogado. Sabendo que aparecem números distintos, ache a probabilidade de que: (*a*) a soma seja par, (*b*) a soma exceda a 9.

7.73 Sejam A e B eventos com $P(A) = 0{,}6$, $P(B) = 0{,}3$ e $P(A \cap B) = 0{,}2$. Ache: (*a*) $P(A \cup B)$; (*b*) $P(A \mid B)$, (*c*) $P(B \mid A)$.

7.74 Sejam A e B eventos com $P(A) = \frac{1}{3}$, $P(B) = \frac{1}{4}$ e $P(A \cup B) = \frac{1}{2}$. (*a*) Ache $P(A \mid B)$ e $P(B \mid A)$. (*b*) A e B são independentes?

7.75 Sejam A e B eventos com $P(A) = 0{,}3$, $P(A \cup B) = 0{,}5$ e $P(B) = p$. Ache p se:

(*a*) A e B forem mutuamente disjuntos; (*b*) A e B forem independentes; (*c*) A for subconjunto de B.

7.76 Sejam A e B eventos independentes com $P(A) = 0{,}3$ e $P(B) = 0{,}4$. Ache: (*a*) $P(A \cap B)$ e $P(A \cup B)$; (*b*) $P(A \mid B)$ e $P(B \mid A)$.

7.77 Em um clube, 60% dos membros jogam tênis, 40% jogam golfe e 205 jogam ambos, tênis e golfe. Um membro é escolhido aleatoriamente.

(*a*) Ache a probabilidade de que ele não jogue nem golfe nem tênis.

(*b*) Se ele joga tênis, ache a probabilidade de que jogue golfe.

(*c*) Se ele joga golfe, ache a probabilidade de que jogue tênis.

7.78 A caixa A contém seis bolas de gude vermelhas e duas azuis, e a caixa B contém duas vermelhas e quatro azuis. Uma bola é aleatoriamente retirada de cada caixa.

(*a*) Ache a probabilidade p de que ambas as bolas sejam vermelhas.

(*b*) Ache a probabilidade p de que uma bola seja vermelha e a outra, azul.

7.79 A probabilidade de que A atinja o alvo é $\frac{1}{4}$, e a probabilidade de que B atinja o alvo é $\frac{1}{3}$.

(*a*) Se cada um atirar duas vezes, qual é a probabilidade de que o alvo seja atingido pelo menos uma vez?

(*b*) Se cada um atirar uma vez e o alvo for atingido apenas uma vez, qual é a probabilidade de que A tenha acertado o alvo?

7.80 Três moedas confiáveis são lançadas. Considere os eventos:

$$A = \{\text{só caras ou só coroas}\}, \quad B = \{\text{pelo menos duas caras}\}, \quad C = \{\text{no máximo duas caras}\}$$

Dentre os pares (A, B), (A, C) e (B, C), quais são independentes? Quais são dependentes?

Tentativas Repetidas e Distribuição Binomial

7.81 Sempre que os cavalos a, b e c correm juntos, suas respectivas probabilidades de vitória são 0,3, 0,5 e 0,2. Eles correm juntos três vezes.

(*a*) Ache a probabilidade de que o mesmo cavalo ganhe os três páreos.

(*b*) Ache a probabilidade de que cada um dos cavalos a, b e c tenha uma vitória.

7.82 A média do número de acertos com o taco de um jogador de baseball é 0,3. Ele se coloca para jogar com o taco quatro vezes. Ache a probabilidade de que ele acerte: (*a*) exatamente uma vez; (*b*) pelo menos uma vez.

7.83 A probabilidade com que Antônio acerta um lance de três pontos no basquete é $p = 0{,}4$. Ele tenta $n = 5$ vezes. Ache a probabilidade de que acerte: (*a*) exatamente duas vezes; (*b*) pelo menos uma vez.

7.84 Um time vence (V) com probabilidade 0,5, perde (P) com probabilidade 0,3 e empata (E) com probabilidade 0,2. O time joga duas vezes. (*a*) Determine o espaço amostral S e a probabilidade de cada evento elementar. (*b*) Ache a probabilidade de que o time vença pelo menos uma vez.

7.85 Um certo tipo de míssil atinge o alvo com probabilidade $p = \frac{1}{3}$. (*a*) Se três mísseis são lançados, ache a probabilidade de que o alvo seja atingido pelo menos uma vez. (*b*) Ache o número de mísseis que devem ser lançados para que se tenha pelo menos 90% de probabilidade de atingir o alvo.

Variáveis Aleatórias

7.86 Um par de dados é lançado. Seja X o mínimo dos dois números que ocorrem. Ache a distribuição e a expectância de X.

7.87 Uma moeda confiável é jogada quatro vezes. Seja X o maior *string* de caras. Ache a distribuição e a expectância de X.

7.88 Uma moeda com uma distribuição de massa tal que $P(H) = \frac{1}{3}$ e $P(T) = \frac{1}{2}$ é lançada até que uma cara ou cinco coroas ocorram. Ache o número esperado de lançamentos da moeda.

7.89 A probabilidade de que um time A ganhe algum jogo é $\frac{1}{2}$. Suponha que A jogue com B em um torneio. O primeiro time que ganhar dois jogos seguidos ou três jogos ganha o torneio. Ache o número esperado de jogos no torneio.

7.90 Uma caixa contém 10 transistores dos quais dois têm defeitos. É selecionado e testado um transistor até que seja escolhido um sem defeitos. Ache o número esperado de transistores a serem escolhidos.

7.91 Um jogo de loteria com 500 cupons dá um prêmio de \$ 100, três prêmios de \$ 50 e cinco prêmios de \$ 25. (*a*) Ache o valor esperado para a vitória de um cupom. (*b*) Se um cupom custa \$ 1, qual o valor esperado do jogo?

7.92 Um jogador lança três moedas confiáveis. Ele ganha \$ 5 se três caras ocorrerem, \$ 3 se ocorrerem duas caras e \$ 1 se apenas uma cara ocorrer. Por outro lado, ele perde \$ 15 se ocorrerem três coroas. Ache o valor do jogo para o jogador.

Média, Variância e Desvio-Padrão

7.93 Ache a média μ, a variância σ^2 e o desvio-padrão σ de cada distribuição:

(*a*)

x_i	2	3	8
p_i	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

(*b*)

x_i	−1	0	1	2	3
p_i	0,3	0,1	0,1	0,3	0,2

7.94 Ache a média μ, a variância σ^2 e o desvio-padrão σ da seguinte distribuição de dois pontos, com $p + q = 1$:

x_i	a	b
$f(x_i)$	p	q

7.95 Duas cartas são selecionadas de uma caixa que contém cinco cartões numerados 1, 1, 2, 2 e 3. Sejam X a soma e Y o máximo dos dois números retirados. Ache a distribuição, a média, a variância e o desvio-padrão das variável aleatórias: (*a*) X; (*b*) Y; (*c*) $Z = X + Y$; (*d*) $W = XY$. (Veja o Problema 7.49 para a definição de $Z = X + Y$ e $W = XY$.)

7.96 O time A tem probabilidade $p = 0{,}8$ de ganhar a cada vez que joga. Seja X o número de vezes que A ganhará em $n = 100$ jogos. Ache a média μ, a variância σ^2 e o desvio-padrão σ de X.

7.97 Um estudante mal preparado faz um teste de cinco questões do tipo "verdadeiro ou falso" tentando adivinhar todas as respostas. Ache a probabilidade de o estudante passar se o critério de aprovação for o de que se obtenha pelo menos quatro respostas corretas.

7.98 Seja X uma variável aleatória com distribuição binomial $B(n, p)$ com $E(X) = 2$ e $\text{Var}(X) = \frac{8}{5}$. Ache n e p.

Respostas dos Problemas Complementares

7.53 (*a*) $A \cup B^c$; (*b*) $A \cap B^c$.

7.54 (*a*) $A \cap B \cap C^c$; (*b*) $(A \cup C) \cap B$; (*c*) $(A \cup B \cup B)^c = A^c \cap B^c \cap C^c$; (*d*) $(A \cap B) \cup (A \cap C) \cup (B \cap C)$.

7.55 (*a*) $n(S) = 24$; $S = \{H, T\} \times \{H, T\} \times \{1, 2, \ldots, 6\}$.
(*b*) $A = \{HH2, HH4, HH6\}$; $B = \{HH2, HT2, TH2, TT2\}$;
$C = \{HT1, HT3, HT5, TH1, TH3, TH5\}$.
(*c*) (i) HH2; (ii) HT2, TH2, TT2; (iii) $\varnothing$.

7.56 (*a*) $\frac{5}{6}$; (*b*) $\frac{15}{16}$; (*c*) $\frac{30}{36}$.

7.57 (*a*) $\frac{8}{18}$; (*b*) $\frac{3}{18}$; (*c*) $\frac{5}{18}$.

7.58 (*a*) $\frac{40}{50}$; (*b*) $\frac{10}{50}$; (*c*) $\frac{8}{150}$; (*d*) $\frac{42}{50}$.

7.59 (*a*) $\frac{1}{13}$; (*b*) $\frac{7}{13}$; (*c*) $\frac{8}{13}$; (*d*) $\frac{7}{13}$.

7.60 (*a*) $\frac{3}{10}$; (*b*) $\frac{3}{10}$; (*c*) $\frac{1}{13}$; (*d*) $\frac{8}{13}$.

7.61 $\frac{3}{5}$.

7.62 $\frac{1}{3}$.

7.63 (*a*) 3/4; (*b*) $\frac{1}{4}$; (*c*) $\frac{1}{3}$; (*d*) $\frac{7}{12}$.

7.64 (*a*) $[4(3!)(3!)]/6! = \frac{1}{5}$; (*b*) $[2(3!)(3!)]/6! = \frac{1}{10}$.

7.65 (*c*) e (*d*).

7.66 $P(H) = \frac{3}{4}$; $P(T) = \frac{1}{4}$.

7.67 (*a*) $\frac{2}{3}$; (*b*) $\frac{1}{3}$; (*c*) $\frac{3}{5}$.

7.68 (*a*) 0,6, 0,8, 0,5; (*b*) 0,5, 0,7, 0,4.

7.69 (*a*) 0,3; (*b*) 0,8; (*c*) 0,2; (*d*) 0,2.

7.70 (*a*) 0,5; (*b*) 0,1; (*c*) 0,2; (*d*) 0,5.

7.71 (*a*) $\frac{1}{6}, \frac{5}{6}$; (*b*) $\frac{1}{2}, \frac{1}{3}$; (*c*) $\frac{1}{2}, \frac{5}{9}$; (*d*) $\frac{1}{2}, 1$; (*e*) sim, sim, não.

7.72 (*a*) $\frac{12}{30}$; (*b*) $\frac{4}{30}$.

7.73 (*a*) 0,7; (*b*) $\frac{2}{3}$; (*c*) $\frac{1}{3}$.

7.74 (*a*) $\frac{1}{3}, \frac{1}{4}$; (*b*) sim.

7.75 (*a*) 0,2; (*b*) $\frac{2}{9}$; (*c*) 0,5.

7.76 (*a*) 0,12, 0,58; (*b*) $\frac{3}{10}$, $\frac{4}{10}$.

7.77 (*a*) 20%; (*b*) $\frac{1}{3}$; (*c*) $\frac{1}{2}$.

7.78 (*a*) $\frac{1}{4}$; (*b*) $\frac{7}{12}$.

7.79 (*a*) $\frac{3}{4}$; (*b*) $\frac{1}{3}$.

7.80 Apenas (A, B).

7.81 (*a*) 0,16; (*b*) 0,18.

7.82 (*a*) $6(0,3)^2(0,7)^2 = 0,2646$, (*b*) $1 - (0,7)^4 = 0,7599$.

7.83 (*a*) $10(0,4)^2(0,6)^3 = 0,2646$; (*b*) $1 - (0,6)^5 = 0,7599$.

7.84 (*b*) P(VV, VE, EV) = 0,55.

7.85 (*a*) $1 - \left(\frac{2}{3}\right)^3 = \frac{19}{27}$; (*b*) cinco vezes.

7.86

x_i	1	2	3	4	5	6
p_i	$\frac{11}{36}$	$\frac{9}{36}$	$\frac{7}{36}$	$\frac{5}{36}$	$\frac{3}{36}$	$\frac{1}{36}$

$E(X) = \frac{91}{36} \approx 2,5$.

7.87

x_i	0	1	2	3	4
p_i	$\frac{1}{16}$	$\frac{7}{16}$	$\frac{5}{16}$	$\frac{2}{16}$	$\frac{1}{16}$

$E(X) = \frac{27}{16} \approx 1,7$.

7.88 $\frac{211}{81} \approx 2,6$.

7.89 $\frac{23}{8} \approx 2,9$.

7.90 $\frac{11}{9} \approx 1,2$.

7.91 (*a*) 0,75; (*b*) − 0,25.

7.92 0,25.

7.93 (*a*) $\mu = 4$, $\sigma^2 = 5,5$, $\sigma = 2,3$; (*b*) $\mu = 1$, $\sigma^2 = 2,4$, $\sigma = 1,5$.

7.94 $\mu = ap + bq$; $\sigma^2 = pq(a - b)^2$; $\sigma = |a - b|\sqrt{pq}$.

7.95 (*a*)

x_i	2	3	4	5
$P(x_i)$	0,1	0,4	0,3	0,2

$E(X) = 3{,}6$; $\text{Var}(X) = 0{,}84$; $\sigma_X = 0{,}9$.

(*b*)

y_j	1	2	3
$P(y_j)$	0,1	0,5	0,4

$E(Y) = 2{,}3$; $\text{Var}(Y) = 0{,}41$; $\sigma_Y = 0{,}64$.

(*c*)

z_k	3	5	6	7	8
$P(z_k)$	0,1	0,4	0,1	0,2	0,2

$E(Z) = 5{,}9$; $\text{Var}(Z) = 2{,}3$; $\sigma_Z = 1{,}5$.

(*d*)

w_k	2	6	8	12	15
$P(w_k)$	0,1	0,4	0,1	0,2	0,2

$E(W) = 8{,}8$; $\text{Var}(W) = 17{,}6$; $\sigma_W = 4{,}2$.

7.96 $\mu = 80$; $\sigma^2 = 16$; $\sigma = 4$.

7.97 $\frac{6}{32} = \frac{3}{16}$.

7.98 $n = 6$; $p = \frac{1}{3}$.

Capítulo 8

Teoria dos Grafos

8.1 INTRODUÇÃO, ESTRUTURAS DE DADOS

Grafos, grafos orientados, árvores e árvores binárias estão presentes em muitas áreas da matemática e da ciência d computação. Este e os próximos dois capítulos cobrirão esses tópicos. Entretanto, a fim de entender como esses ob jetos podem ser armazenados na memória e para entender os algoritmos que os manipulam, necessitamos saber ur pouco a respeito de certas estruturas. Assumimos que o leitor entenda *arrays* lineares e bidimensionais; portanto discutiremos abaixo apenas listas ligadas e ponteiros[†] e pilhas e filas.

Listas Ligadas e Ponteiros

Listas ligadas e ponteiros serão apresentados por meio de um exemplo. Suponha que uma firma de corretagem man tém um arquivo em que cada registro contém o nome do cliente e um corretor; digamos que o arquivo contém o seguintes dados:

Cliente	Abreu	Batista	Cunha	Duarte	Escobar	Fonseca	Gomes	Horta	Iglesias
Corretor	Silva	Rocha	Rocha	Jobim	Silva	Jobim	Rocha	Silva	Rocha

Existem duas operações básicas que alguém poderia realizar nos dados:

Operação A: dado o nome do cliente, achar seu corretor.
Operação B: dado o nome do corretor, achar seus clientes.

Discutimos diferentes maneiras pelas quais os dados podem ser armazenados no computador e a facilidade com qu cada uma delas permite a execução das operações *A* e *B* sobre os dados.

Claramente o arquivo pode ser armazenado em um computador em um *array* com duas linhas (ou colunas) d nove nomes. Como os clientes estão listados em ordem alfabética, pode-se facilmente executar a operação *A*. En tretanto, para executar a operação *B*, é preciso realizar uma busca em todo o *array*.

Pode-se facilmente armazenar os dados na memória usando um *array* bidimensional onde, por exemplo, as li nhas correspondam à lista alfabética de clientes, e as colunas correspondam à lista alfabética de corretores, e colo cando 1 na matriz para indicar o corretor de um cliente e 0 nas demais posições. O maior problema desta represen tação é que pode ocorrer desperdício de área de memória, porque podem aparecer muitos zeros na matriz.

[†] N. de T. No original, *pointers*, por vezes também chamados de apontadores. Alguns textos usam o nome "ponteiro" quando o valor é fixo, "apontador", quando é variável.

Por exemplo, em uma firma com 1000 clientes e 20 corretores, seriam necessárias 20 000 posições de memória para os dados, mas apenas 1000 dentre elas seriam significativas.

Discutimos abaixo uma forma de armazenar os dados na memória que usa listas ligadas e ponteiros. Por *listas ligadas*, designamos uma coleção linear de elementos de dados, chamados *nós*, onde a ordem é dada por meio de um campo com um ponteiro. A Figura 8-1 é um diagrama esquemático de uma lista ligada com seis nós. Isto é, cada nó é dividido em duas partes: a primeira contém a informação daquele elemento (por exemplo, NOME, ENDEREÇO,...), e a segunda parte, chamada *campo com o endereço* ou *apontador para o próximo*[†], contém o endereço do próximo nó da lista. Esse apontador é indicado por uma seta desenhada de um nó para o próximo nó da lista. Também existe um ponteiro variável, chamado de START na Figura 8-1, que tem o endereço do primeiro nó da lista. Além disso, o apontador do último nó da lista, chamado *apontador nulo*, contém um endereço inválido que indica o final da lista.

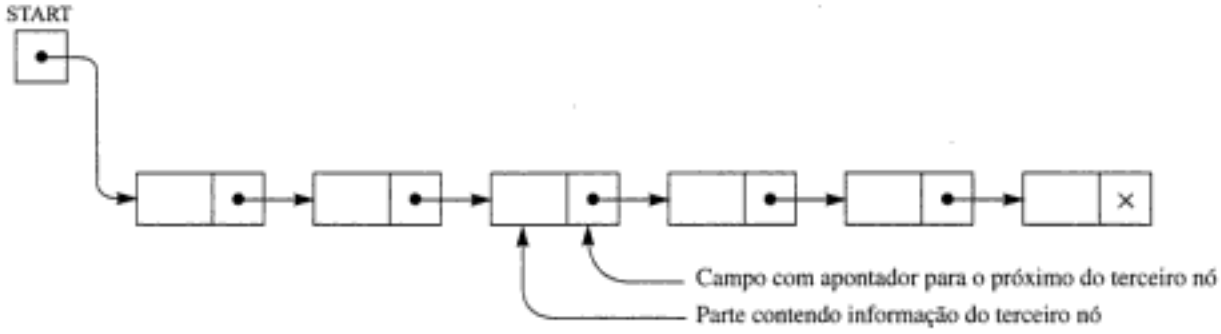


Fig. 8-1 Lista ligada com seis nós.

Uma maneira importante de armazenar o dado original, indicada na Figura 8-2, usa listas ligadas. Observe que existem *arrays* separados (ordenados alfabeticamente) para os clientes e os corretores. Também, existe um *array* de ponteiros CORR paralelo a CLIENTE que indica a localização do corretor de um cliente; portanto, a operação *A* pode ser executada de forma fácil e rápida. Ademais, a lista de clientes de cada corretor é uma lista ligada, como discutido acima. Especificamente, existe um *array* de ponteiros, START, paralelo a CORRETOR, que aponta para o primeiro cliente de um corretor, e existe um *array* PROX que aponta para a localização do próximo cliente na lista de corretores (ou contém um 0 para indicar o final da lista). Esse processo está indicado pelas setas na Figura 8-2 para o corretor Rocha.

	Cliente	CORR	PROX
1	Abreu	3	5
2	Batista	2	3
3	Cunha	2	7
4	Duarte	1	6
5	Escobar	3	8
6	Fonseca	1	0
7	Gomes	2	9
8	Horta	3	0
9	Iglesias	2	0

Corretor	START	
Jobim	4	1
Rocha	2	2
Silva	1	4

Fig. 8-2

A operação *B* pode agora ser executada fácil e rapidamente; isto é, não é preciso procurar em toda a lista de clientes para obter a lista de clientes de um determinado corretor. A seguir, temos a descrição do algoritmo para este processo (escrito em pseudocódigo).

[†] N. de T. No original, *link field* ou *nextpointer field*.

Algoritmo 8.1 Lê o nome do corretor e imprime a lista de seus clientes.

Passo 1 Leia XXX.

Passo 2 Ache K tal que CORRETOR[K] = XXX [Use busca binária.]

Passo 3 Faça PTR := START[K] [Inicializa o ponteiro PTR.]

Passo 4 Repita enquanto PTR ≠ NULL.

(a) Imprima CLIENTE[PTR].

(b) Faça PTR := PROX[PTR]. [Atualiza PTR.]

[Fim do *loop*.]

Passo 5 Saia.

Pilhas, Filas e Filas de Prioridades

Existem estruturas de dados diferentes de *arrays* e listas ligadas que aparecem nos nossos algoritmos sobre grafos. Essas estruturas, filas, pilhas e filas de prioridades estão descritas superficialmente abaixo.

(a) ***Pilha***: uma *pilha*, também conhecida como um sistema *last-in first-out* (LIFO)† é uma lista linear onde inserções e deleções só podem ocorrer em uma única extremidade, chamada "topo" da lista. Esta estrutura é semelhante, no que diz respeito a suas operações, a uma pilha de pratos, como representado na Figura 8-3(a). Note que um novo prato é inserido apenas no topo da pilha e pratos só podem ser retirados do topo da pilha.

(a) Pilha de pratos (b) Fila esperando pelo ônibus

Fig. 8-3

(b) ***Fila***: uma *fila*, também conhecida como um sistema *first-in first-out* (FIFO)††, é uma lista linear em que deleções só podem ocorrer em uma extremidade (a "frente" da lista) e inserções só podem ocorrer na outra extremidade da lista (a "parte de trás" da lista), como representado na Figura 8-3(b). Isto é, a primeira pessoa na fila é a primeira pessoa a embarcar no ônibus, e uma pessoa recém-chegada vai para o final da fila.

(c) ***Filas de prioridades***: seja S um conjunto de elementos onde novos elementos podem ser periodicamente inseridos, mas, a cada momento, o elemento que for maior (elemento com "maior prioridade") será deletado. Então, S é dito uma fila de prioridades. As regras "mulheres e crianças primeiro" e "idade antes de beleza" são exemplos de filas de prioridades. Pilhas e filas comuns são tipos especiais de filas de prioridades. Especificamente, o elemento com a maior prioridade numa pilha é o último elemento inserido, mas o elemento com maior prioridade em uma fila é o primeiro elemento inserido.

8.2 GRAFOS E MULTIGRAFOS

Um *grafo* G consiste em duas coisas:

(i) Um conjunto $V = V(G)$ cujos elementos são chamados *vértices*, *pontos* ou *nós* de G.

(ii) Um conjunto $E = E(G)$ de pares não ordenados de vértices distintos, chamados *arestas* de G†††.

† N. de T. Em geral não é traduzido; tem o sentido de "último a chegar, primeiro a sair".

†† N. de T. Em geral não é traduzido; tem o sentido de "primeiro a chegar, primeiro a sair".

††† N. de T. A letra E vem de *edges*. Textos em português usam, por vezes, o símbolo aG em vez de $E(G)$.

Denotamos um tal grafo por $G(V, E)$ quando queremos enfatizar as duas partes de G.

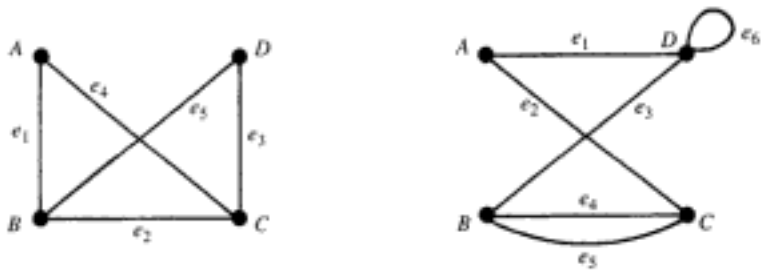
Vértices u e v são ditos adjacentes se existe uma aresta $e = \{u, v\}$. Neste caso, u e v são ditos os *extremos* de e, e diz-se que e *conecta* u a v. Além disso, diz-se que uma aresta e é *incidente* a seus extremos u e v.

Grafos são representados por diagramas no plano de modo natural. Especificamente, cada vértice v em V é representado por um ponto (ou pequeno círculo), e cada aresta $e = \{v_1, v_2\}$ é representada por uma curva que conecta seus extremos v_1 e v_2. Por exemplo, a Figura 8-4(a) representa o grafo $G(V, E)$ onde:

(i) V consiste nos vértices A, B, C, D.

(ii) E consiste nas arestas $e_1 = \{A, B\}$, $e_2 = \{B, C\}$, $e_3 = \{C, D\}$, $e_4 = \{A, C\}$, $e_5 = \{B, D\}$.

Na prática, usaremos mais freqüentemente o desenho do diagrama de um grafo para representá-lo do que uma lista explícita de seus vértices.



(a) Grafo (b) Multigrafo

Fig. 8-4

Multigrafos

Considere o diagrama da Figura 8-4(b). As arestas e_4 e e_5 são ditas *arestas múltiplas*, já que conectam os mesmos extremos, e a aresta e_6 é dita um *laço*, uma vez que seus extremos são o mesmo vértice. Um diagrama deste tipo é dito um *multigrafo*. A definição formal de grafo não permite nem arestas múltiplas nem laços. Portanto, um grafo pode ser definido como sendo um multigrafo sem arestas múltiplas ou laços.

Observação: Alguns textos usam o termo *grafo* incluindo multigrafo, e o termo *grafo simples* para um grafo sem arestas múltiplas ou laços.

Grau de um Vértice

O grau de um vértice v em um grafo G (escreve-se $\deg(v)$[†]) é igual ao número de arestas em G que contém v, isto é, que são incidentes a v. Como cada aresta é contada duas vezes na contagem dos graus dos vértices de G, temos o seguinte resultado simples, mas importante.

Teorema 8-1: a soma dos graus dos vértices de um garfo G é igual a duas vezes o número de arestas em G.

Considere, por exemplo, o grafo da Figura 8-4(a). Temos

$$\deg(A) = 2, \qquad \deg(B) = 3, \qquad \deg(C) = 3, \qquad \deg(D) = 2$$

A soma dos graus é igual a 10, que, como esperado, é igual a duas vezes o número de arestas. Um vértice é dito *par* ou *ímpar* dependendo de o seu grau ser um número par ou ímpar. Portanto, A e D são vértices pares, enquanto B e C são vértices ímpares.

O Teorema 8.1 também vale para multigrafos onde um laço é contado duas vezes para efeito do cálculo do grau de seus extremos. Por exemplo, na Figura 8-4(b), temos $\deg(D) = 4$, já que a aresta e_6 é contada duas vezes; portanto, D é um vértice ímpar.

Um vértice de grau zero é dito um vértice *isolado*.

[†] N. de T. Do inglês *degree*; em português, também se usa $g\,G(v)$.

Grafos Finitos e Grafo Trivial

Um multigrafo é dito *finito* se tem um número finito de vértices e um número finito de arestas. Observe que um grafo com um número finito de vértices deve ter, automaticamente, um número finito de arestas e, portanto, é finito. O grafo finito com um vértice e nenhuma aresta, i.e., um único ponto, é dito o *grafo trivial*. A menos que afirmação em contrário seja feita, os multigrafos neste livro serão finitos.

8.3 SUBGRAFOS, GRAFOS ISOMORFOS E HOMEOMORFOS

Esta seção discutirá relações importantes entre grafos.

Subgrafos

Considere um grafo $G = G(V, E)$. Um grafo $H = H(V', E')$ é dito um *subgrafo* de G se os vértices e as arestas de H estão contidos nos vértices e arestas de G, isto é, $V' \subseteq V$ e $E' \subseteq E$. Em particular:

(i) Um subgrafo $H(V', E')$ de $G(V, E)$ é dito um subgrafo *induzido* pelos seus vértices V' se o seu conjunto de arestas E' contém todas as arestas em G cujos extremos pertencem a vértices em H.

(ii) Se v é um vértice em G, então $G - v$ é o subgrafo de G obtido deletando v de G e deletando todas as arestas em G que contêm V.

(iii) Se e é uma aresta em G, $G - e$ é o subgrafo de G obtido deletando a aresta e de G.

Grafos Isomorfos

Os grafos $G(V, E)$ e $G^*(V^*, E^*)$ são ditos *isomorfos* se existe uma correspondência bijetora $f: V \to V^*$ tal que $\{u, v\}$ é uma aresta de G se e somente se $\{f(u), f(v)\}$ é uma aresta de G^*. Normalmente não distinguimos grafos isomorfos (ainda que seus diagramas pareçam distintos). A Figura 8-5 mostra 10 grafos desenhados como letras. Notamos que A e R são grafos isomorfos. F e T, K e X, e M, S, V e Z são grafos isomorfos.

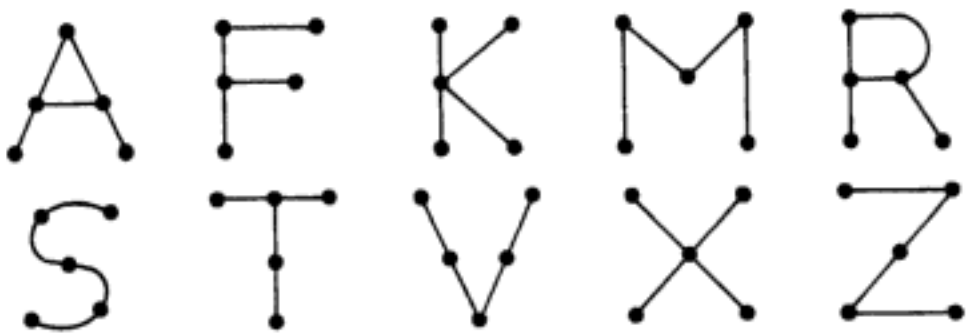


Fig. 8-5

Grafos Homeomorfos

Dado um grafo qualquer G, podemos obter um novo grafo dividindo uma aresta de G com vértices adicionais. Dois grafos G e G^* são ditos *homeomorfos* se puderem ser obtidos a partir de um mesmo grafo ou de grafos isomorfos por este método. Os grafos (a) e (b) na Figura 8-6 não são isomorfos, mas são homeomorfos, já que podem ser obtidos do grafo (c) pela adição dos vértices apropriados.

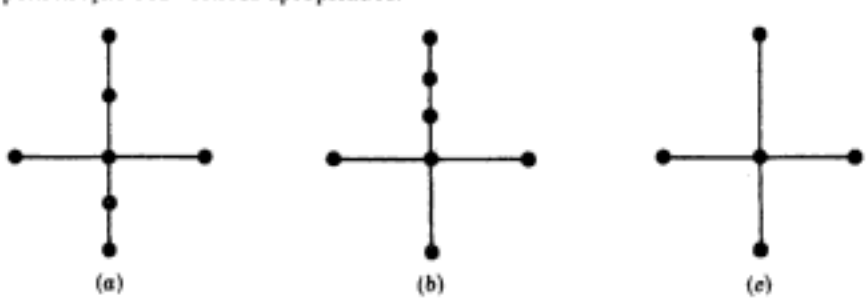


Fig. 8-6

8.4 CAMINHOS E CONECTIVIDADE

Um *caminho* em um multigrafo G consiste em uma seqüência alternada de vértices e arestas da forma

$$v_0, \quad e_1, \quad v_1, \quad e_2, \quad v_2, \quad \ldots, \quad e_{n-1}, \quad v_{n-1}, \quad e_n, \quad v_n$$

onde cada aresta e_i contém os vértices v_{i-1} e v_i (que aparecem dos dois lados de e_i na seqüência). O número n de arestas é dito o *comprimento* do caminho. Quando não houver possibilidade de ambigüidades, denotamos um caminho por sua seqüência de vértices. O caminho é dito *fechado* se $v_0 = v_n$. Caso contrário, dizemos que o caminho é de v_0 para v_n, ou *entre* v_0 e v_n, ou que *conecta* v_0 a v_n.

Um *caminho simples* é um caminho em que todos os vértices são distintos[†]. (Um caminho em que todas as arestas são distintas é chamado *trilha*.) Um *ciclo* é um caminho fechado de comprimento 3 ou mais onde todos os vértices são distintos, exceto $v_0 = v_n$. Um ciclo de comprimento k é chamado de *k-ciclo*.

Exemplo 8.1 Considere o grafo G da Figura 8-7(a). Considere as seguintes seqüências:

$$\alpha = (P_4, P_1, P_2, P_5, P_1, P_2, P_3, P_6), \qquad \beta = (P_4, P_1, P_5, P_2, P_6),$$
$$\gamma = (P_4, P_1, P_5, P_2, P_3, P_5, P_6), \qquad \delta = (P_4, P_1, P_5, P_3, P_6).$$

A seqüência α é um caminho de P_4 para P_6; porém, não é uma trilha, já que a aresta $\{P_1, P_2\}$ é usada duas vezes. A seqüência β não é um caminho, já que não existe aresta $\{P_2, P_6\}$. A seqüência γ é uma trilha, uma vez que nenhuma aresta é usada duas vezes; mas não é um caminho simples, pois o vértice P_5 é usado duas vezes. A seqüência δ é um caminho simples de P_4 para P_6; mas não é o menor caminho (no que diz respeito ao comprimento) de P_4 para P_6. O menor caminho de P_4 a P_6 é o caminho simples (P_4, P_5, P_6), que tem comprimento 2.

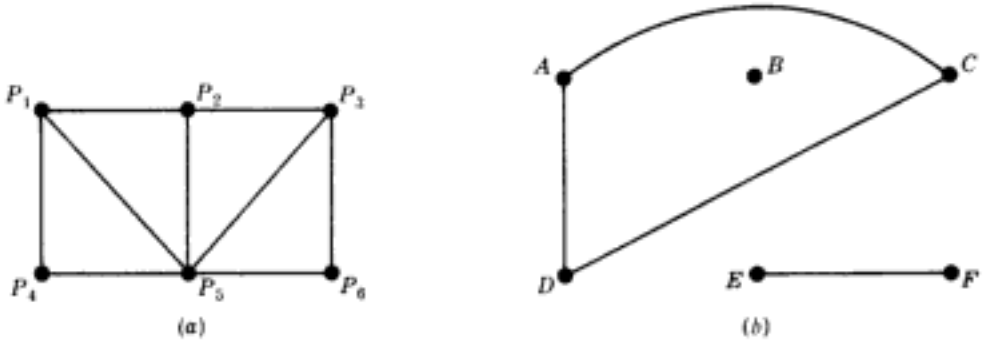


Fig. 8-7

Eliminando arestas desnecessárias, não é difícil ver que qualquer caminho de um vértice u para um vértice v pode ser substituído por um caminho simples de u para v. Afirmamos formalmente esse resultado.

Teorema 8-2: existe um caminho de um vértice u para um vértice v se e somente se existe um caminho simples de u para v.

Conectividade e Componentes Conexas

Um grafo G é *conexo* se existe um caminho entre quaisquer dois dos seus vértices. O grafo da Figura 8-7(a) é conexo, mas o grafo da Figura 8-7(b) não é conexo, uma vez que, por exemplo, não existe caminho entre os vértices D e E.

Suponha que G é um grafo. Um subgrafo conexo H de G é chamado *componente conexa* de G se H não está contido em nenhum outro subgrafo conexo de G. Intuitivamente é claro que qualquer garfo G pode ser particionado nas suas componentes conexas. Por exemplo, o grafo G da Figura 8-7(b) tem três componentes conexas: os subgrafos induzidos pelos conjuntos de vértices $\{A, C, D\}$, $\{E, F\}$ e $\{B\}$.

O vértice B da Figura 8-7(b) é chamado de *vértice isolado*, já que B não pertence a nenhuma aresta, ou, em outras palavras, deg $(B) = 0$. Portanto, como observado, o próprio B forma uma componente conexa do grafo.

[†] N. de T. Alguns textos usam a palavra "passeio" para caminhos, reservando o termo "caminho" para o caso de vértices distintos.

Observação: De um ponto de vista formal, assumindo que todo vértice u é conectado a si mesmo, a relação "u está conectado a v" é uma relação de equivalência no conjunto de vértices de um grafo G e as classes de equivalência induzidas pela relação são as componentes conexas de G.

Distância e Diâmetro

Considere um grafo conexo G. A *distância* entre os vértices u e v em G (denota-se $d(u, v)$) é o comprimento do menor caminho entre u e v. O *diâmetro* de G (denota-se diam (G)) é o máximo da distância entre quaisquer dois pontos de G. Por exemplo, na Figura 8-8(a), $d(A,F) = 2$ e diam$(G) = 3$, enquanto na Figura 8-8(b), $d(A, F) = 3$ e diam$(G) = 4$.

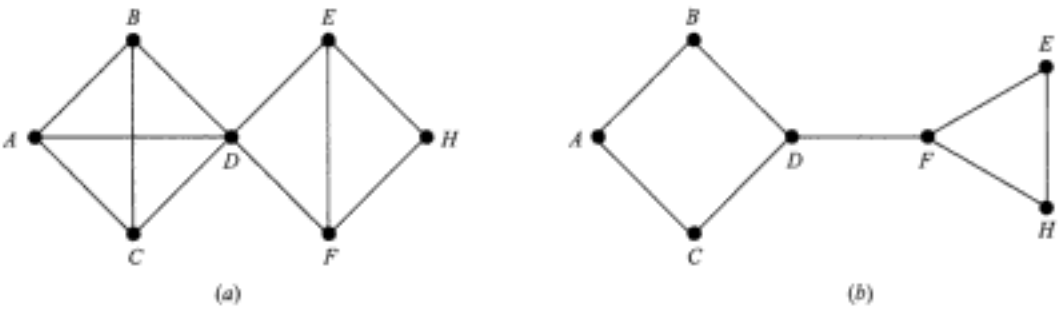


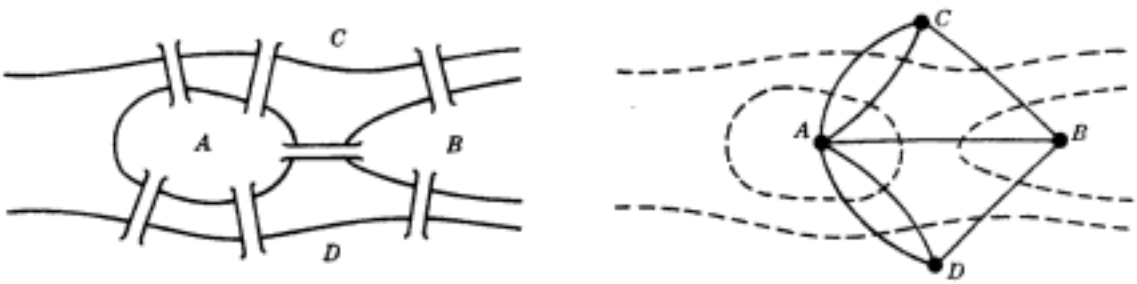
Fig. 8-8

Cortes e Conexões

Seja G um grafo conexo. Um vértice v em G é dito um *corte* se $G - v$ é desconexo. (Lembre que $G - v$ é o grafo obtido de G pela deleção de v e das arestas que contêm v.) Uma aresta e de G é dita uma *conexão* se $G - e$ é desconexo. (Lembre que $G - e$ é o grafo obtido de G pela simples deleção da aresta e.) Na Figura 8-8(a), o vértice D é um corte e não existem conexões. Na Figura 8-8(b), a aresta $e = \{D, F\}$ é uma conexão. (Seus extremos, D e F, são necessariamente cortes.)

8.5 AS PONTES DE KÖNISBERG E MULTIGRAFOS ATRAVESSÁVEIS

A cidade de Könisberg, no leste da Prússia, no século 18 incluía duas ilhas e sete pontes, como mostrado na Figura 8-9(a). Pergunta: saindo de qualquer lugar e chegando a qualquer lugar, uma pessoa pode andar pela cidade cruzando as sete pontes sem atravessar nenhuma delas duas vezes? O povo de Könisberg escreveu ao famoso matemático suíço L. Euler a este respeito. Euler provou, em 1736, que tal percurso era impossível. Ele trocou as ilhas e os dois lados do rio por pontos, e as pontes, por curvas, obtendo a Figura 8-9(b).



(a) Könisberg em 1736 (b) Representação gráfica de Euler

Fig. 8-9

Observe que a Figura 8-9(*b*) é um multigrafo. Um multigrafo é dito *atravessável*† se "pode ser desenhado sem quebras nas curvas e sem repetição de arestas", isto é, se existe um caminho que inclua todos os vértices e use cada aresta exatamente uma vez. Um tal caminho deve ser uma trilha (já que nenhuma aresta é usada duas vezes) e será chamado uma *trilha atravessável*. Claramente, um multigrafo atravessável precisa ser finito e conexo. A Figura 8-10(*b*) mostra a trilha atravessável do multigrafo na Figura 8-10(*a*). (Para indicar a direção da trilha, o diagrama interrompe o traço nos vértices que são realmente visitados.) Não é difícil ver que a caminhada em Könisberg é possível se e somente se o multigrafo da Figura 8-9(*b*) é atravessável.

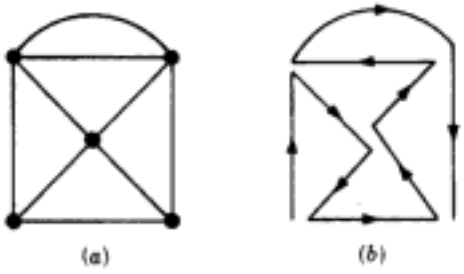


Fig. 8-10

Mostramos agora como Euler provou que o multigrafo da Figura 8-9(*b*) não é atravessável e, portanto, a caminhada em Könisberg é impossível. Lembre primeiramente que um vértice é par ou ímpar dependendo de o seu grau ser um número par ou ímpar. Suponha que um multigrafo é atravessável e que em um dado vértice P não comece nem termine uma trilha atravessável. Afirmamos que P é um vértice ímpar. De fato, sempre que uma trilha atravessável chega em P por uma aresta, deve existir uma aresta ainda não usada pela qual a trilha pode sair de P. Portanto, as arestas na trilha incidentes a P devem aparecer aos pares, e, portanto, P é um vértice par. Logo, se um vértice Q é ímpar, a trilha atravessável precisa começar ou terminar em Q. Conseqüentemente, um multigrafo com mais de dois vértices ímpares não pode ser atravessável. Observe que o multigrafo correspondente ao problema das pontes de Könisberg tem quatro vértices ímpares. Logo, não se pode caminhar por Könisberg de forma que cada ponte seja percorrida exatamente uma vez.

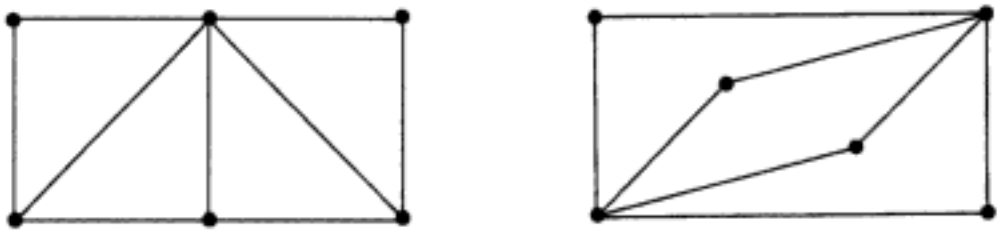
Euler de fato provou o converso da afirmação acima, que está contida no teorema e corolário seguintes. (O teorema está provado no Problema 8.9.) Um grafo G é dito um grafo *euleriano* se existe uma trilha atravessável fechada, chamada trilha *euleriana*.

Teorema 8-3: (**Euler**) um grafo conexo finito é euleriano se e somente se cada vértice tem grau par.

Corolário 8-4: qualquer grafo conexo finito com dois vértices ímpares é atravessável. Uma trilha atravessável pode começar em qualquer vértice ímpar e terminar no outro vértice ímpar.

Grafos Hamiltonianos

A discussão acima sobre grafos eulerianos enfatiza o modo de percorrer arestas; neste ponto, nos concentramos na visita de vértices. Um *circuito hamiltoniano* em um grafo G, assim denominado por causa do matemático irlandês do século 19 William Hamilton (1805-1865), é um caminho fechado que visita todo vértice em G exatamente uma vez. (Um caminho fechado com tais características deve ser um ciclo.) Se G admite um circuito hamiltoniano, então G é dito um *grafo hamiltoniano*. Note que um circuito euleriano percorre cada aresta exatamente uma vez, podendo, entretanto, repetir vértices, enquanto um circuito hamiltoniano visita cada vértice exatamente uma vez, e podendo repetir arestas. A Figura 8-11 mostra um exemplo de grafo que é hamiltoniano mas não euleriano, e vice-versa.



(*a*) Hamiltoniano (*b*) Não euleriano

Fig. 8-11

† N. de T. No original, *transversable*.

Embora seja claro que apenas grafos conexos podem ser hamiltonianos, não existe um critério simples que nos diga se um grafo é ou não hamiltoniano, como no caso dos grafos eulerianos. Temos a seguinte condição suficiente, de G. A. Dirac.

Teorema 8-5: seja G um grafo conexo com n vértices. Então G é hamiltoniano se $n \geq 3$ e $n \leq \deg(v)$ para cada vértice v em G.

8.6 GRAFOS ROTULADOS E PONDERADOS

Um grafo G é dito um *grafo rotulado* se estão associados dados de algum tipo às suas arestas e/ou vértices. Em particular, G é um *grafo ponderado* se a cada aresta e de G está associado um número não negativo $w(e)$ dito o *peso* ou *comprimento* de v. A Figura 8-12 mostra um grafo ponderado onde o comprimento de cada aresta está descrito da maneira óbvia. O *peso* ou *comprimento* de uma caminho em um grafo ponderado G é definido como sendo a soma dos pesos das arestas no caminho. Um problema importante na teoria dos grafos é achar o *menor caminho*, isto é, um caminho de peso (comprimento) mínimo entre quaisquer dois vértices dados. O comprimento do caminho mínimo entre P e Q na Figura 8-12 é 14; um tal caminho é

$$(P, A_1, A_2, A_5, A_3, A_6, Q)$$

O leitor pode tentar determinar um outro caminho mínimo.

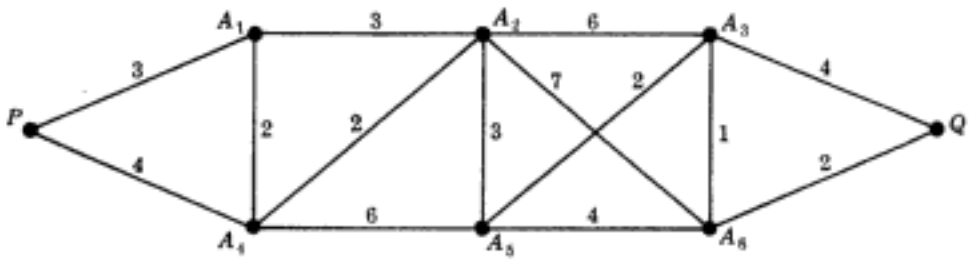


Fig. 8-12

8.7 GRAFOS COMPLETOS REGULARES E BIPARTICIONADOS

Existem muitos tipos diferentes de grafos. Esta seção considera três deles: completos, regulares e biparticionados.

Grafos Completos

Um grafo G é dito *completo* se todo vértice em G está conectado a qualquer outro vértice em G. Portanto, um grafo completo precisa ser conexo. O grafo completo com n vértices é denotado por K_n. A Figura 8-13 mostra os grafos K_1 até K_6.

Grafos Regulares

Um grafo G é *regular de grau k* ou *k-regular* se todo vértice tem grau k. Em outras palavras, um grafo é regular se todo vértice tem o mesmo grau.

Os grafos conexos regulares de grau 0, 1 ou 2 podem ser facilmente descritos. O grafo conexo 0-regular é o grafo trivial com um vértice e nenhuma aresta. O grafo conexo 1-regular é o grafo com dois vértices e uma aresta que os conecta. O grafo conexo 2-regular com n vértices é o grafo que consiste em um único n-ciclo.

Veja a Figura 8-14.

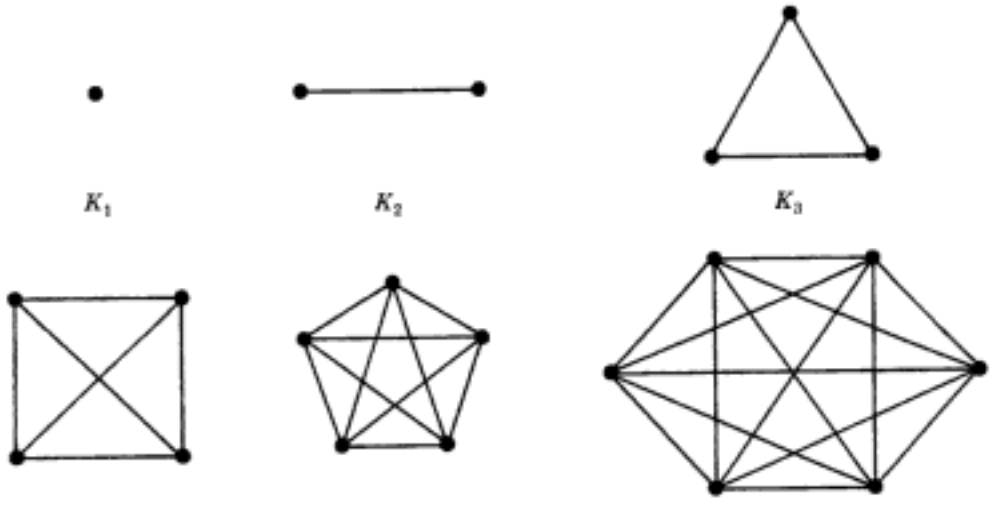
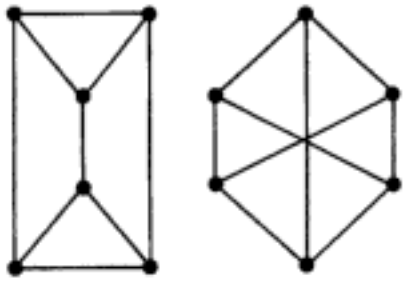


Fig. 8-13

Fig. 8-14 Grafos regulares

Os grafos 3-regulares precisam ter um número par de vértices, já que a soma dos graus dos seus vértices é um número ímpar (Teorema 8.1). A Figura 8-15 mostra dois grafos conexos 3-regulares com seis vértices. Em geral, grafos regulares podem ser bem complicados. Por exemplo, existem 19 grafos 3-regulares com 10 vértices. Notamos que o grafo completo com n vértices K_n é regular de grau $n - 1$.



3-regulares

Fig. 8-15

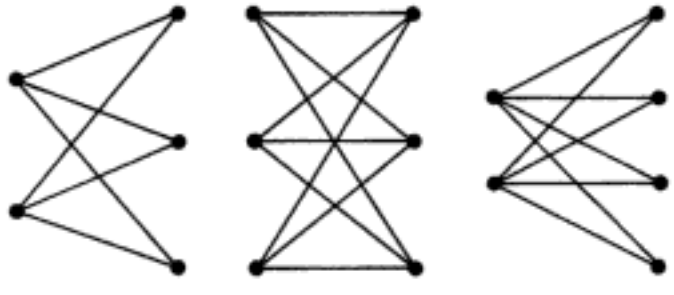


Fig. 8-16

Grafos Biparticionados

Um grafo G é dito *biparticionado* se seu conjunto de vértices V pode ser particionado em dois subconjuntos M e N tais que cada aresta de G conecta um vértice de M a um vértice de N. Chamaremos de completo biparticionado o grafo em que cada vértice de M é conectado a cada vértice de N; esse tipo de grafo é denotado por $K_{m,n}$, onde m é o número de vértices em M, e n é o número de vértices em N, e, para padronizar, vamos assumir $m \leq n$. A Figura 8-16 mostra os grafos $K_{2,3}$, $K_{3,3}$ e $K_{2,4}$. Claramente o grafo $K_{m,n}$ tem mn arestas.

8.8 ÁRVORES

Um grafo T é dito uma *árvore* se T é conexo e não tem ciclos. A Figura 8-17 mostra exemplos de árvores. Uma *floresta* G é um grafo sem ciclos; logo, as componentes conexas de uma floresta são árvores. (Um grafo sem ciclos é dito um grafo *acíclico*.) A árvore que consiste em um único vértice e nenhuma aresta é dita a *árvore degenerada*.

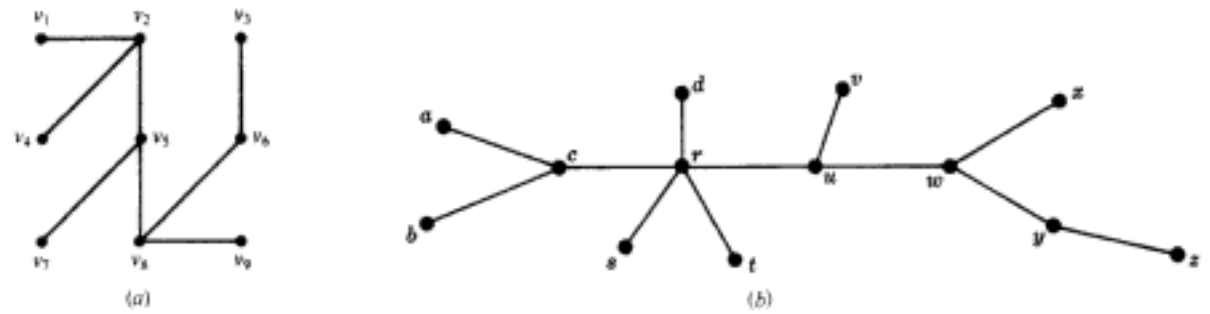


Fig. 8-17

Considere uma árvore T. Claramente, existe apenas um caminho simples entre dois vértices de T; caso contrário, os dois caminhos formariam um ciclo. Além disso:

(*a*) Suponha que não existe uma aresta $\{u, v\}$ em T e adicionamos a aresta $e = \{u, v\}$ a T. Então, o caminho simples de u para v em T e e formará um ciclo; neste caso, T deixará de ser uma árvore.

(*b*) Por outro lado, suponha que existe uma aresta $e = \{u, v\}$ em T e nós deletemos e de T. Então, T não é mais conexo (já que não existe caminho entre u e v); neste caso, T deixa de ser uma árvore.

O seguinte teorema (provado no Problema 8.16) é aplicável quando o grafo é finito.

Teorema 8-6: seja G um grafo com $n > 1$ vértices. Então, as seguintes afirmações são equivalentes:

(i) G é uma árvore.

(ii) G é um grafo acíclico e tem $n - 1$ arestas.

(iii) G é conexo e tem $n - 1$ arestas.

Este teorema também nos diz que um árvore finita T com n vértices precisa ter $n - 1$ arestas. Por exemplo, a árvore da Figura 8-17(*a*) tem nove vértices e oito arestas, e a árvore da Figura 8-17(*b*) tem 13 vértices e 12 arestas.

Árvores Geradoras

Um subgrafo T de um grafo conexo é dito uma *árvore geradora* de G se T é uma árvore e T inclui todos os vértices de G. A Figura 8-18 mostra um grafo conexo G e as árvores geradoras T_1, T_2 e T_3 de G.

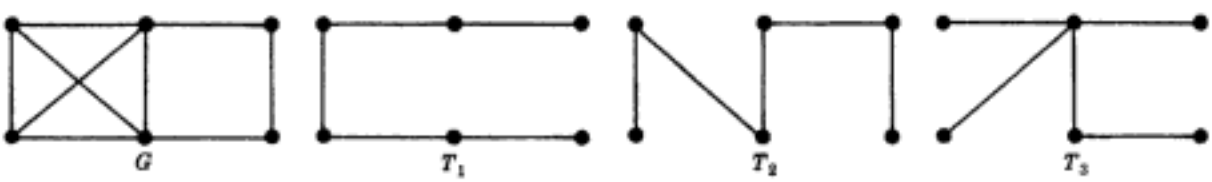


Fig. 8-18

Árvores Geradoras Mínimas

Suponha que G é um grafo conexo ponderado. Isto é, cada aresta de G está associada a um número não negativo chamado *peso* da aresta. Então, qualquer árvore geradora T de G está associada a um peso total obtido pela soma dos pesos das arestas em T. Uma *árvore minimal geradora* de G é uma árvore geradora cujo peso total é o menor possível.

Os Algoritmos 8.8A e 8.8B, a seguir, nos permitem achar a árvore minimal geradora T de um grafo conexo ponderado G, onde G tem n vértices. (Neste caso, T deve ter $n - 1$ arestas.)

Algoritmo 8.8A: A entrada é um grafo conexo ponderado G com n vértices.

Passo 1 Ordene as arestas de G em ordem decrescente de peso.

Passo 2 Seqüencialmente, delete cada aresta que não desconecta o grafo até que restem $n - 1$ arestas.

Passo 3 Saia.

Algoritmo 8.8B: (Kruskal) A entrada é um grafo conexo ponderado G com n vértices.

Passo 1 Ordene as arestas de G em ordem crescente de peso.

Passo 2 Começando apenas com vértices de G e procedendo seqüencialmente, adicione cada aresta que não gere um ciclo até que $n - 1$ arestas sejam adicionadas.

Passo 3 Saia.

O peso de uma árvore minimal geradora é único, mas a árvore, propriamente dita, não é. Árvores geradoras minimais distintas podem ocorrer quando duas ou mais arestas têm o mesmo peso. Neste caso, a ordenação das arestas no Passo 1 dos Algoritmos 8.8A e 8.8B não é única e pode, portanto, resultar em diferentes árvores geradoras minimais como ilustrado no exemplo seguinte.

Exemplo 8.2 Ache uma árvore minimal geradora do grafo ponderado Q da Figura 8-19(a). Note que Q tem seis vértices; logo, uma árvore minimal geradora terá cinco arestas.

(a) Aplicamos aqui o Algoritmo 8.8A.
Primeiramente ordenamos as arestas em ordem decrescente de peso, então sucessivamente deletamos arestas sem desconectar Q até que restem cinco arestas. Disto resultam os dados seguintes:

Arestas	BC	AF	AC	BE	CE	BF	AE	DF	BD
Peso	8	7	7	7	6	5	4	4	3
Deletar?	Sim	Sim	Sim	Não	Não	Sim			

Portanto, a árvore minimal geradora de Q obtida contém as arestas

$$BE,\quad CE,\quad AE,\quad DF,\quad BD$$

A árvore geradora tem peso 24 e é mostrada na Figura 8-19(b).

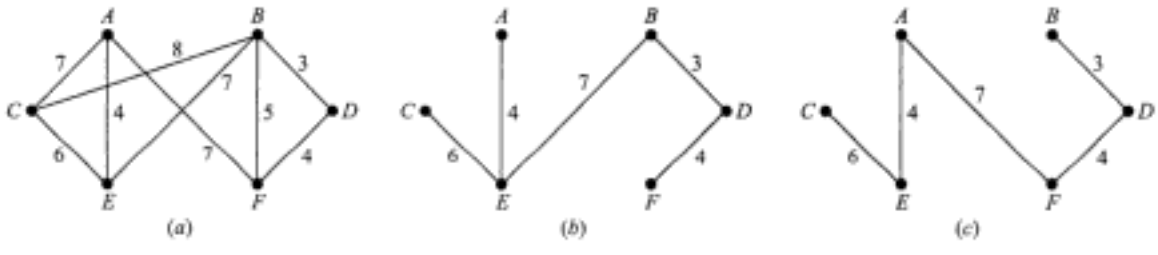


Fig. 8-19

(*b*) Aplicamos aqui o Algoritmo 8.8B.
Primeiramente ordenamos as arestas em ordem crescente de peso; adicionamos então arestas sucessivamente sem formar ciclos, até que cinco arestas sejam incluídas.
Disto resultam os dados seguintes:

Arestas	BD	AE	DF	BF	CE	AC	AF	BE	BC
Peso	3	4	4	5	6	7	7	7	8
Somar?	Sim	Sim	Sim	Não	Sim	Não	Sim		

Portanto, a árvore minimal geradora de Q obtida contém as arestas

$$BD,\quad AE,\quad DF,\quad CE,\quad AF$$

A árvore geradora aparece na Figura 8-19(*c*). Observe que esta árvore geradora não é a mesma que a obtida usando o Algoritmo 8.8A.

Observação: Os algoritmos acima são executados facilmente quando o grafo G é relativamente pequeno, como na Figura 8-19(*a*). Suponha que G tem dúzias de vértices e centenas de arestas que, digamos, são dados por uma lista de pares de vértices. Neste caso, não é óbvio nem mesmo decidir se G é conexo. Pode ser necessário algum tipo de algoritmo de busca em profundidade (DFS – *depth-first search*) ou em largura[†] (BFS – *breath-first search*) em grafos. As seções subseqüentes e o próximo capítulo discutirão maneiras de representar grafos G na memória e vários algoritmos para grafos.

8.9 GRAFOS PLANARES

Um grafo ou multigrafo que pode ser desenhado no plano de tal modo que suas arestas não se cortam é dito *planar*. Embora o grafo completo com quatro vértices K_4 seja normalmente representado com cruzamento de arestas como na Figura 8-20(*a*), ele também pode ser desenhado sem cruzamento de arestas como na Figura 8-20(*b*); portanto K_4 é planar. Árvores formam uma classe importante de grafos planares. Esta seção apresenta a nosso leitor estes importantes grafos.

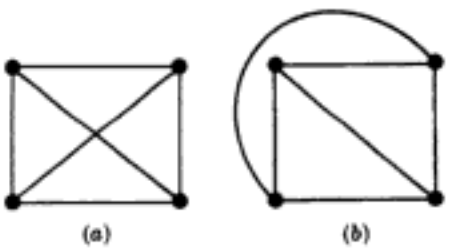


Fig. 8-20

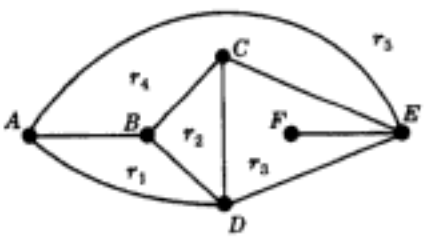


Fig. 8-21

Mapas e Regiões

Uma representação particular planar de um multigrafo planar finito é dita um *mapa*. Dizemos que um mapa é *conexo* se o multigrafo subjacente é conexo. Um determinado mapa divide o plano em várias regiões. Por exemplo, o mapa na Figura 8-21 com seis vértices e nove arestas divide o plano em cinco regiões. Observe que quatro das regiões são limitadas, mas a quinta região, fora do diagrama, não é limitada. Portanto, não há perda de generalidade em contar o número de regiões, admitindo que o nosso mapa está contido em algum retângulo maior, e não no plano inteiro.

[†] N. de T. Também chamada de busca em amplitude.

Observe que o bordo de cada região de um mapa consiste em arestas. Às vezes, as arestas formam um ciclo, mas às vezes não. Por exemplo, na Figura 8-21, os bordos de todas as regiões são ciclos, à exceção de r_3. Entretanto, se nos movermos no sentido horário ao longo de r_3 saindo, por exemplo, do vértice C, obtemos o caminho fechado

$$(C, D, E, F, E, C)$$

onde a aresta $\{E, F\}$ aparece duas vezes. Designamos por *grau* de uma região r, escrevendo $\deg(r)$, o comprimento do ciclo ou do caminho fechado que forma o bordo de r. Notamos que cada aresta é bordo de duas regiões, ou está contida em uma região, e aparece duas vezes em qualquer caminho ao longo do bordo da região. Por conseguinte, temos o teorema para regiões que é análogo ao Teorema 8.1 para vértices.

Teorema 8-7: a soma dos graus das regiões de um mapa é igual a duas vezes o número de arestas.

Os graus das regiões da Figura 8-21 são:

$$\deg(r_1) = 3, \qquad \deg(r_2) = 3, \qquad \deg(r_3) = 5, \qquad \deg(r_4) = 4, \qquad \deg(r_5) = 3$$

A soma dos graus é 18, que é, como esperado, duas vezes o número de arestas.

Por conveniência de notação, vamos desenhar os vértices de um mapa como pontos ou pequenos círculos, ou vamos assumir que quaisquer interseções de linhas ou curvas no plano são vértices.

Fórmula de Euler

Euler apresentou a fórmula que associa o número de vértices V, o número de arestas E e o número de regiões R de qualquer mapa conexo. Especificamente:

Teorema 8-8: **(Euler)** $V - E + R = 2$.

(A demonstração do Teorema 8.8 aparece no Problema 8.20.)

Observe que, na Figura 8-21, $V = 6$, $E = 9$ e $R = 5$; e, como esperado, pela fórmula de Euler,

$$V - E + R = 6 - 9 + 5 = 2$$

Enfatizamos que o grafo subjacente a um mapa deve ser conexo para que a fórmula de Euler seja válida.

Seja G um multigrafo conexo planar com três ou mais vértices, de tal forma que G não é K_1 ou K_2. Seja M uma representação planar de G. Não é difícil ver que (1) uma região de M só pode ter grau 1 se o seu bordo é um laço, e (2) uma região de M pode ter grau 2 apenas se seu bordo consiste em duas arestas múltiplas. Conseqüentemente, se G for um grafo, e não um multigrafo, então toda região de M precisa ter grau maior ou igual a 3. Esse comentário, juntamente com a fórmula de Euler, é usado para provar o resultado seguinte sobre grafos planares.

Teorema 8-9: seja G um grafo planar conexo com p vértices e p arestas, onde $p \geq 3$. Então, $q \geq 3p - 6$.

Note que o teorema não é verdade para K_1, onde $p = 1$ e $q = 0$, e não é verdade para K_2, onde $p = 2$ e $q = 1$.

Demonstração: Seja r o número de regiões em uma representação planar de G. Pela fórmula de Euler,

$$p - q + r = 2$$

Note que a soma dos graus das regiões é igual a $2q$ pelo Teorema 8.7. Mas cada região tem grau maior ou igual a 3. Portanto,

$$2q \geq 3r$$

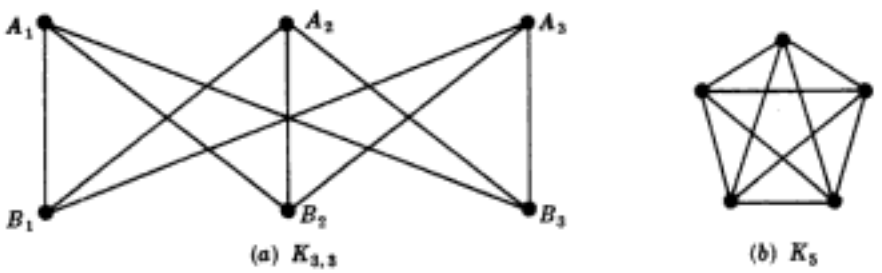
Logo, $r \geq 2q/3$. Substituindo na fórmula de Euler, obtém-se

$$2 = p - q + r \leq p - q + \frac{2q}{3} \qquad \text{ou} \qquad 2 \leq p - \frac{q}{3}$$

A multiplicação da desigualdade por 3 dá $6 \leq 3p - q$, que é o resultado procurado.

Grafos não Planares e Teorema de Kuratowski

Exibimos dois exemplos de grafos não planares. Considere primeiro o *utility graph*[†]; isto é, três casas A_1, A_2 e A_3 devem ser conectadas a saídas para água, gás e eletricidade B_1, B_2 e B_3 como na Figura 8-22(*a*). Observe que este é o grafo $K_{3,3}$ que tem $p = 6$ vértices e $q = 9$ arestas. Suponha que o grafo é planar. Pela fórmula de Euler, uma representação planar tem $r = 5$ regiões. Observe que nenhuma tripla de vértices está conectada entre si; portanto, o grau de cada região deve ser maior ou igual a 4 e, portanto, a soma dos graus das regiões deve ser maior ou igual a 20. Pelo Teorema 8.9, o grafo deve ter 10 ou mais arestas. Isto contradiz o fato de que o grafo tem $q = 9$ arestas. Portanto, o *utility graph* é não planar.



(*a*) $K_{3,3}$ (*b*) K_5

Fig. 8-22

Considere a seguir o *grafo estrela* da Figura 8-22(*b*). Este é o grafo completo K_5 com $p = 5$ vértices que tem $q = 10$ arestas. Se o grafo é planar, pelo Teorema 8.9,

$$10 = q \leq 3p - 6 = 15 - 6 = 9$$

o que é impossível. Portanto, K_5 não é planar.

Por muitos anos, os matemáticos tentaram caracterizar grafos planares e não planares. Esse problema foi finalmente resolvido em 1930 pelo matemático polonês K. Kuratowski. A demonstração deste resultado, enunciado abaixo, está além do objetivo deste texto.

Teorema 8-10: **(Kuratowski)** um grafo é não planar se e somente se contém um subgrafo homeomorfo a $K_{3,3}$ ou K_5.

8.10 COLORAÇÃO DE GRAFOS

Considere um grafo G. Uma *coloração de vértices* ou, simplesmente, uma *coloração* de G é uma atribuição de cores aos vértices de G de tal forma que vértices adjacentes têm cores distintas. Dizemos que G é n-colorável se existe uma coloração de G que usa n cores. O número mínimo de cores necessárias para pintar G é dito o *número cromático* de G e é denotado por $\chi(G)$.

Apresentamos um algoritmo de Welch e Powell para a coloração de um grafo G. Enfatizamos que o algoritmo nem sempre fornece a coloração minimal de G.

Algoritmo 8.10: (Welch-Powell) A entrada é um grafo G.

Passo 1 Ordene os vértices de G em ordem decrescente de grau.

Passo 2 Atribua a primeira cor, C_1, ao primeiro vértice e, então, seqüencialmente, atribua C_1 a cada vértice que não é adjacente a algum vértice que o antecedeu e ao qual foi atribuída a cor C_1.

Passo 3 Repita o Passo 2 com a segunda cor C_2 e os vértices subseqüentes não coloridos.

Passo 4 Repita o Passo 3 com a terceira cor C_3, depois com a quarta cor C_4, e assim por diante, até que todos os vértices estejam coloridos.

Passo 5 Saia.

[†] N. de T. Optamos por manter a expressão em inglês por não ter tradução consagrada.

Exemplo 8.3

(*a*) Considere o grafo *G* da Figura 8-23. Usamos o algoritmo de Welch-Powell para obter uma coloração de *G*. Ordenando em ordem decrescente de grau, obtém-se a seqüência seguinte:

$$A_5, \quad A_3, \quad A_7, \quad A_1, \quad A_2, \quad A_4, \quad A_6, \quad A_8$$

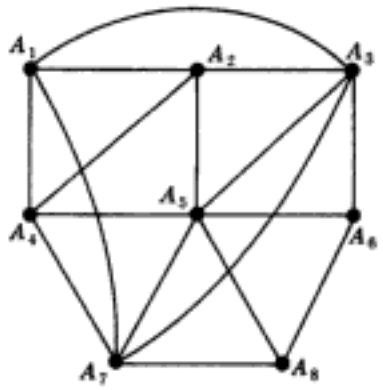


Fig. 8-23

A primeira cor é atribuída aos vértices A_5 e A_1. A segunda cor é atribuída aos vértices A_3, A_4 e A_8. A terceira cor é atribuída aos vértices A_7, A_2 e A_6. Todos os vértices receberam uma cor, e, logo, *G* é 3-colorável. Observe que *G* não é 2-colorável, já que os vértices A_1, A_2 e A_3, que estão conectados entre si, precisam receber cores diferentes. Conseqüentemente, $\chi(G) = 3$.

(*b*) Considere o grafo completo K_n com *n* vértices. Como todo vértice é adjacente a qualquer outro vértice, K_n requer *n* cores em qualquer coloração. Logo, $\chi(K_n) = n$.

Não existe uma maneira simples de determinar realmente quando um grafo arbitrário é *n*-colorável. Entretanto, o teorema seguinte (provado no Problema 8.22) apresenta uma caracterização simples de grafos 2-coloráveis.

Teorema 8-11: as seguintes afirmações são equivalentes para um grafo *G*:

(i) *G* é 2-colorável.

(ii) *G* é biparticionado.

(iii) Todo ciclo de *G* tem grau ímpar.

Não existe limite no número de cores que podem ser necessárias para a coloração de um grafo arbitrário, uma vez que, por exemplo, o grafo completo K_n requer *n* cores. Entretanto, se nos restringirmos aos grafos planares, não importa qual seja o número de vértices, cinco cores são suficientes. Especificamente, no Problema 8.24, provamos:

Teorema 8-12: qualquer grafo planar é 5-colorável.

De fato, desde 1950 os matemáticos têm conjecturado que grafos planares são 4-coloráveis já que todo o grafo planar conhecido é 4-colorável. Kenneth Appel e Wofgang Haken mostraram finalmente, em 1976, que esta conjectura era verdadeira. Isto é:

Teorema das Quatro Cores (Appel e Haken): Todo grafo planar é 4-colorável.

Discutimos esse teorema na próxima subseção.

Mapas Duais e o Teorema das Quatro Cores

Considere um mapa *M*, digamos o mapa *M* da Figura 8-24(*a*). Em outras palavras, *M* é uma representação planar de um multigrafo planar. Duas regiões de *M* são ditas *adjacentes* se elas têm uma aresta em comum. Portanto, as regiões r_2 e r_5 da Figura 8-24(*a*) são adjacentes, mas as regiões r_3 e r_5 não são. Uma *coloração* de *M* é uma associação de uma cor a cada região de *M* tal que regiões adjacentes têm cores distintas. Um mapa *M* é *n*-colorável se existe uma coloração de *M* que tem *n* cores. Portanto, o mapa *M* da Figura 8-24(*a*) é 3-colorável, já que as regiões podem ser associadas às seguintes cores:

r_1 vermelho, r_2 branco, r_3 vermelho, r_4 branco, r_5 vermelho, r_6 azul

Observe a semelhança entre a presente discussão sobre coloração de mapas e a discussão anterior sobre coloração de grafos. De fato, usando o conceito de mapa dual, definido abaixo, pode-se mostrar que a coloração de um mapa é equivalente à coloração de vértice de um grafo planar.

Considere um mapa M. Em cada região de M escolhemos um ponto e, se duas regiões têm uma aresta em comum, conectamos os pontos correspondentes com uma curva que intercepta a aresta comum. Essas curvas podem ser desenhadas de maneira que não se interceptem. Então, obtemos um novo mapa M^*, chamado *dual* de M, tal que cada vértice de M^* corresponde a exatamente uma região de M. A Figura 8-24(b) mostra o mapa dual da Figura 8-24(a). Pode-se mostrar que cada região de M^* conterá exatamente um vértice de M, e que cada aresta de M^* vai interceptar exatamente uma aresta de M e vice-versa. Assim, M será o mapa dual de M^*.

Observe que qualquer coloração das regiões de um mapa M corresponderá a uma coloração dos vértices do mapa dual M^*. Logo, M é n-colorável se e somente se o grafo planar do mapa dual M^* é n-colorável nos vértices. Assim, o teorema anterior pode ser reescrito como a seguir:

Teorema das Quatro Cores (Appel e Haken): se as regiões de qualquer mapa M são coloridas de forma que regiões adjacentes têm cores distintas, então não mais do que quatro cores são necessárias.

A demonstração do teorema acima utiliza computadores, essencialmente. Especificamente, Appel e Haken mostraram primeiramente que, se o teorema das quatro cores fosse falso, deveria existir um contra-exemplo em um conjunto de aproximadamente 2000 grafos planares. Mostraram depois, usando o computador, que nenhum destes tipos de grafos planares era um contra-exemplo. A análise de cada tipo diferente de grafo parece estar além do alcance de seres humanos sem o uso do computador. Assim, a demonstração, diferentemente da maioria das demonstrações em matemática, depende de tecnologia; isto é, dependeu do desenvolvimento de computadores de alto desempenho.

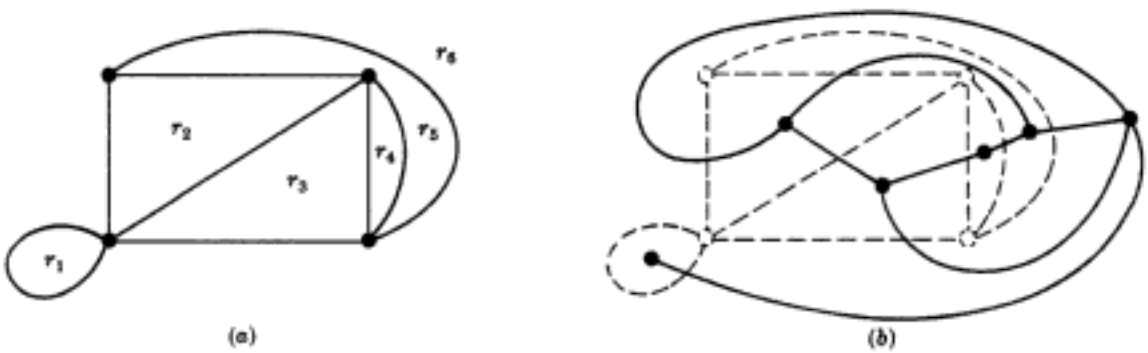


Fig. 8-24

8.11 REPRESENTAÇÃO DE GRAFOS NA MEMÓRIA DE COMPUTADORES

Existem duas maneiras-padrão de manter um grafo na memória de um computador. Uma maneira, chamada *representação seqüencial* de G, é feita através de sua matriz de adjacências A. A outra forma, dita *representação ligada* ou *estrutura de adjacências* de G, usa listas ligadas de vizinhanças. Usualmente, são usadas matrizes quando o grafo G é denso; listas ligadas são mais usadas quando é esparso. (Um grafo G com m vértices e n arestas é dito *denso* quando $m = O(n^2)$, e *esparso* quando $m = O(n)$ ou ainda $O(n \log n)$.)

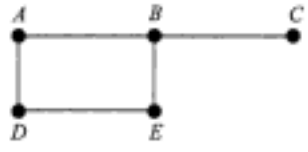
Independentemente da forma como um grafo G é armazenado na memória, normalmente sua entrada no computador é feita através da definição formal, isto é, como uma coleção de vértices e uma coleção de pares de vértices (arestas).

Matriz de Adjacências

Suponha que G é um grafo com m vértices, e suponha que os vértices são ordenados como, digamos, $v_1, v_2, \ldots, v_m$. A matriz de adjacências $A = [a_{ij}]$ do grafo G é a matriz $m \times m$ definida por

$$a_{ij} = \begin{cases} 1 & \text{Se } v_i \text{ é adjacente a } v_j \\ 0 & \text{caso contrário} \end{cases}$$

A Figura 8-25(*b*) contém a matriz de adjacências do grafo G da Figura 8-25(*a*), onde os vértices são ordenados como A, B, C, D, E. Observe que cada vértice $\{v_i, v_j\}$ de G é representado duas vezes, sendo $a_{ij} = 1$ e $a_{ji} = 1$. Portanto, em particular, a matriz de adjacências é simétrica.



(*a*)

	A	B	C	D	E
A	0	1	0	1	0
B	1	0	1	0	1
C	0	1	0	0	0
D	1	0	0	0	1
E	0	1	0	1	0

(*b*)

Fig. 8-25

A matriz de adjacências A de um grafo G depende da ordenação dos vértices de G, isto é, uma ordem diferente dos vértices gera uma matriz de adjacências diferente. Entretanto, quaisquer duas matrizes de adjacências estão intimamente relacionadas, podendo uma ser obtida a partir da outra pela simples troca de posição de linhas e colunas. Por outro lado, a matriz de adjacências não depende da ordem na qual as arestas (pares de vértices) são dadas ao computador.

Existem variações da representação acima. Se G é um multigrafo, normalmente atribuímos a a_{ij} o número de arestas $\{v_i, v_j\}$. Ademais, se G é um grafo ponderado, podemos deixar a_{ij} denotar o peso de $\{v_i, v_j\}$.

Representação Ligada de um Grafo *G*

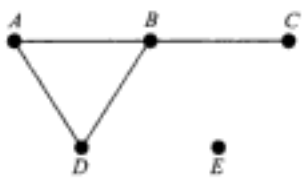
Seja G um grafo com m vértices. A representação de G na memória pela sua matriz de adjacências tem um número considerável de dificuldades. Primeiramente, pode ser difícil inserir ou deletar vértices em G. A razão disso é que pode haver modificações no tamanho de A, e os vértices talvez tenham que ser reordenados, de tal maneira que podem acontecer muitas mudanças na matriz A. Além disto, suponha que o número de arestas é $O(m)$ ou mesmo $O(m \log m)$, isto é, suponha que G é esparso. Então, a matriz A conterá muitos zeros; assim, uma grande quantidade de memória será desperdiçada. Conseqüentemente, quando G é esparso, normalmente G é representado na memória por algum tipo de *representação ligada*, também chamada *estrutura de adjacências*, que está descrita abaixo por um exemplo.

Considere o grafo G da Figura 8-26(*a*). Observe que G pode ser definido de modo equivalente pela tabela da Figura 8-26(*b*), que mostra cada vértice de G seguido por sua *lista de adjacências*, i.e., a lista de vértices adjacentes (*vizinhos*). Aqui, o símbolo $\varnothing$ denota a lista vazia. Essa tabela também pode ser representada em forma compacta

$$G = [A: B, D;\quad B: A, C, D;\quad C: B;\quad D: A, B;\quad E: \varnothing]$$

onde dois-pontos ":" separa um vértice de sua lista de vizinhos, e o ponto-e-vírgula ";" separa listas diferentes.

Observação: Observe que cada aresta do grafo G é representada duas vezes na estrutura de adjacências; isto é, qualquer aresta, por exemplo $\{A, B\}$, é representada por B na lista de adjacências de A e também por A na lista de adjacências de B. O grafo B da Figura 8-26(*a*) tem quatro arestas e, portanto, devem existir oito vértices nas listas de adjacências. Por outro lado, cada vértice da lista de adjacências corresponde a uma única aresta no grafo G.



Vértice	Lista de adjacências
A	*B, D*
B	*A, C, D*
C	*B*
D	*A, B*
E	∅

Fig. 8-26

A *representação ligada* de um grafo G, que mantém G na memória usando suas listas de adjacências, normalmente conterá dois arquivos (ou conjuntos de registros), um chamado de arquivo de vértices e outro chamado de arquivo de arestas, como a seguir.

(*a*) **Arquivo de vértices:** O arquivo de vértices contém a lista de vértices do grafo G normalmente mantida por um *array* ou por uma lista ligada. Cada registro do arquivo de vértices terá a forma

VÉRTICE	PROX-V	PTR	

Aqui, VÉRTICE será o nome do vértice, PROX-V aponta para o próximo vértice na lista de vértices no arquivo de vértices, quando os vértices são mantidos por uma lista ligada, e PTR apontará para o primeiro elemento na lista de adjacências dos vértices que aparecem no arquivo de arestas. A área sombreada indica que pode haver outras informações no registro que corresponde ao vértice.

(*b*) **Arquivo de arestas:** O arquivo de arestas contém as arestas do grafo G. Especificamente, o arquivo de arestas conterá todas as listas de adjacências de G, onde cada lista é mantida na memória por uma lista ligada. Cada registro do arquivo de arestas corresponderá a um vértice na lista de adjacências e, portanto, indiretamente, a uma aresta de G. O registro, normalmente, terá a forma

ARESTA	ADJ	PROX	

Aqui:

(1) ARESTA será o nome da aresta (se houver).
(2) ADJ aponta para a posição do vértice no arquivo de vértices.
(3) PROX aponta para a localização do vértice seguinte na lista de adjacências.

Enfatizamos que cada aresta é repesentada duas vezes no arquivo de arestas, mas cada registro do arquivo corresponde a uma única aresta. A área sombreada indica que pode haver outras informações no registro que corresponde à aresta.

A Figura 8-27 mostra como o grafo G na Figura 8-26(*a*) pode aparecer na memória. Aqui, os vértices de G são mantidos na memória por uma lista ligada usando a variável START para apontar para o primeiro vértice. (Outra alternativa seria usar um *array* linear para a lista de vértices; neste caso, PROX-V não seria necessário.) Note que o campo ARESTA não é necessário aqui, já que as arestas não têm nome. A Figura 8-27 também mostra, por setas, a lista de adjacências [D, C, A] do vértice *B*.

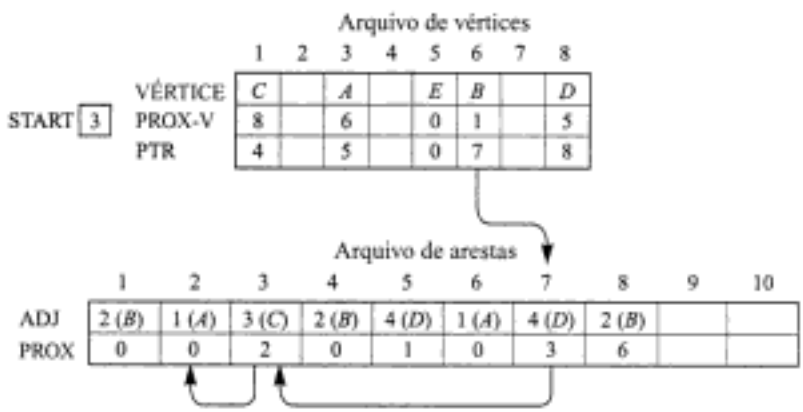
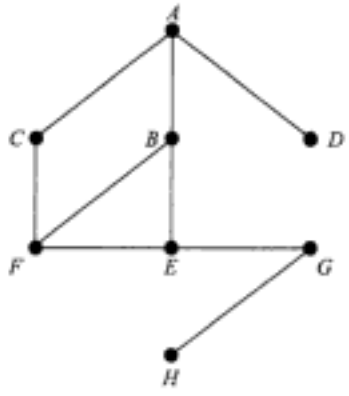


Fig. 8-27

8.12 ALGORITMOS PARA GRAFOS

Esta seção discute dois importantes algoritmos para grafos que examinam sistematicamente os vértices e arestas de um grafo G. Um deles é chamado de *busca em profundidade* (DFS), e o outro é chamado *busca em largura* (BFS). Outros algoritmos para grafos serão discutidos no próximo capítulo, em conexão com grafos orientados. Qualquer algoritmo para grafos pode depender da maneira como G é armazenado na memória. Aqui, assumimos que G é mantido na memória pela sua estrutura de adjacências. Nosso grafo de teste G e sua estrutura de adjacências aparecem na Figura 8-28.



(a)

Vértice	Lista de adjacências
A	*B, C, D*
B	*A, E, F*
C	*A, F*
D	*A*
E	*B, F, G*
F	*B, C, E*
G	*E, H*
H	*G*

(b)

Fig. 8-28

Durante a execução dos nossos algoritmos, cada vértice (nó) *N* de *G* terá um dos seguintes estados, chamados de *status* de *N*, como a seguir

STATUS = 1: (estado de prontidão) o estado inicial de um vértice *N*.
STATUS = 2: (estado de espera) o vértice *N* está numa lista de espera, aguardando para ser processado.
STATUS = 3: (estado processado) o vértice foi processado.

A lista de espera para busca em profundidade será uma PILHA (modificada), enquanto a lista de espera para a busca em largura será uma FILA.

Busca em Profundidade

A idéia geral de uma busca em profundidade começando pelo vértice *A* é descrita a seguir. Primeiramente processamos o vértice *A*. Depois, processamos cada vértice *N* ao longo de um caminho *P* que inicia no vértice *A*; isto é, processamos um vizinho de *A*, depois um vizinho de um vizinho de *A*, e assim por diante. Então, chegamos a um "ponto morto", isto é, um vértice que não tem vizinhos que não estejam processados. Retrocedemos então no caminho *P* até que possamos continuar ao longo de outro caminho *P'*, e assim por diante. O retrocesso é feito usando uma PILHA contendo os vértices inicias de novos possíveis caminhos. Também precisamos de um campo, STATUS, que nos diz o estado corrente de qualquer vértice, de tal forma que nenhum vértice seja processado mais de uma vez. O algoritmo é o seguinte.

Algoritmo 8.12A: **(Busca em profundidade)** Este algoritmo executa uma busca em profundidade em um grafo *G* começando de um vértice de partida *A*.

Passo 1 Inicialize todos os vértices para o estado prontidão (STATUS = 1).

Passo 2 Insira o vértice de partida *A* e mude seu *status* para estado de espera (STATUS = 2).

Passo 3 Repita os Passos 4 e 5 até que a PILHA esteja vazia.

Passo 4 Retire o vértice *N* do topo da PILHA. Processe *N*, faça STATUS (*N*) = 3, o estado processado.

Passo 5 Examine cada vizinhança *J* de *N*.

(a) Se STATUS (*J*) = 1 (estado de prontidão), insira *J* na PILHA e faça STATUS (*J*) = 2 (estado de espera).

(b) Se STATUS (*J*) = 2 (estado de espera), delete o *J* anterior da PILHA e insira o *J* corrente na pilha.

(c) Se STATUS (*J*) = 3 (estado processado), ignore o vértice *J*.

[Fim do *loop* no Passo 3.]

Passo 6 Saia.

O algoritmo acima irá processar apenas os vértices que estão conectados ao vértice de partida *A*, isto é, as componentes conexas incluindo *A*. Suponha que se queira processar todos os vértices no grafo *G*. Então, o algoritmo precisa ser modificado de tal forma que recomece de um novo vértice (que chamaremos de *B*) que ainda esteja no estado de prontidão (STATUS = 1). Esse vértice *B* pode ser obtido percorrendo a lista de vértices.

Observação: A estrutura PILHA no algoritmo anterior não é tecnicamente uma pilha, uma vez que, no Passo 5(*b*), permitimos que um vértice *J* seja deletado e posteriormente inserido no topo da pilha. (Embora ele seja o mesmo vértice *J*, representa normalmente uma aresta diferente na estrutura de adjacências.) Se não movermos *J* no Passo 5(*b*), obteremos uma forma alternada para o algoritmo de busca em profundidade.

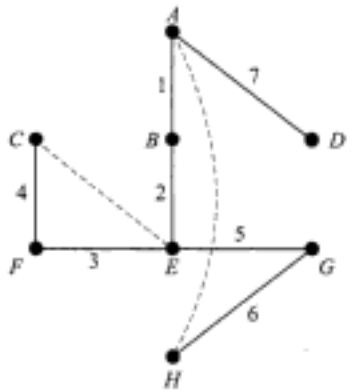
Exemplo 8.4 Suponha que o Algoritmo 8-12A é aplicado ao grafo da Figura 8-28. Os vértices são processados na seguinte ordem:

$$A, \quad B, \quad E, \quad F, \quad C, \quad G, \quad H, \quad D$$

Especificamente, a Figura 8-29(*a*) mostra a seqüência de listas de espera em PILHA e os vértices em processamento. Usamos a barra / para indicar que um vértice é deletado da fila de espera. Cada vértice, excluindo *A*, vem de uma lista de adjacências e corresponde, portanto, a uma aresta do grafo. Essas arestas formam uma árvore geradora de *G*, que está representada na Figura 8-29(*b*). Os números indicam a ordem das arestas a serem adicionadas à árvore, e as linhas tracejadas indicam a reversão do sentido em que o caminho é percorrido.

Vértice	PILHAS
	A
A	*B*, *C*, *D*
B	*E*, *F*, *C*, *D*
E	*F*, *G*, *F*, *C*, *D*
F	*C*, *G*, *E*, *D*
C	*G*, *D*
G	*H*, *D*
H	*D*
D	

(*a*)



(*b*)

Fig. 8-29

Busca em Largura

A idéia geral por trás de uma busca em largura que começa com um vértice de partida *A* é descrita a seguir. Primeiramente processamos o vértice de partida *A*. Depois, processamos todos os vizinhos de *A*, e assim sucessivamente. Naturalmente precisamos ter o controle dos vizinhos de um vértice, e precisamos garantir também que nenhum vértice seja processado duas vezes. Isto é feito usando FILA para conhecer os vértices que aguardam processamento, e pelo campo STATUS que nos indica o *status* corrente de um vértice. O algoritmo vem a seguir.

Algoritmo 8.12B: **(Busca em largura)**: Este algoritmo executa a busca em largura em um Grafo *G* começando com um vértice de partida *A*.

Passo 1 Inicialize todos os vértices para o estado de prontidão (STATUS = 1).

Passo 2 Coloque o vértice de partida *A* em FILA e mude seu *status* para estado de espera (STATUS = 2).

Passo 3 Repita os Passos 4 e 5 até que FILA esteja vazia.

Passo 4 Remova o vértice *N* na frente da FILA. Processe *N*, faça STATUS (*N*) = 3, o estado processado.

Passo 5 Examine cada vizinhança *J* de *N*.

(a) Se STATUS (*J*) = 1(estado de prontidão), coloque *J* no final de FILA e faça STATUS (*J*) = 2 (estado de espera).

(b) Se STATUS (*J*) = 2 (estado de espera), ou STATUS (*J*) = 3 (processado), ignore o vértice *J*. [Fim do *loop* no Passo 3.]

Passo 6 Saia.

Novamente, o algoritmo acima irá processar apenas os vértices que estão conectados ao vértice de partida *A*, isto é, as componentes conexas incluindo *A*. Suponha que se queira processar todos os vértices no grafo *G*. Então, o algoritmo precisa ser modificado de tal forma que recomece de um novo vértice (que chamaremos de *B*) que ainda esteja no estado de prontidão (STATUS = 1). Este vértice *B* pode ser obtido percorrendo a lista de vértices.

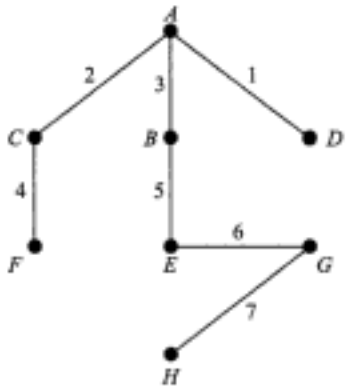
Exemplo 8.5 Suponha que o algoritmo 8.12B é aplicado ao grafo da Figura 8-28. Os vértices são processados na seguinte ordem:

$$A, \quad D, \quad C, \quad B, \quad F, \quad E, \quad G, \quad H$$

Especificamente, a Figura 8-30(*a*) mostra a seqüência de listas de espera em FILA e os vértices em processamento. Novamente, cada vértice, excluindo A, vem de uma lista de adjacências e, portanto, corresponde a uma aresta do grafo. Essas adjacências formam uma árvore geradora de G, que está representada na Figura 8-30(*b*). De novo, o número indica a ordem em que as arestas são adicionadas à árvore. Observe que essa árvore geradora é diferente daquela da Figura 8-29(*b*), proveniente do algoritmo de busca em profundidade.

Vértice	FILA
	A
A	B, C, D
D	B, C
C	$F, B,$
B	E, F
F	E
E	G
G	H
H	

(*a*)



(*b*)

Fig. 8-30

Problemas Resolvidos

Terminologia de Grafos

8.1 Considere a Figura 8-31. (*a*) Descreva formalmente o grafo G do diagrama, isto é, ache o conjunto $V(G)$ de vértices de G e o conjunto $E(G)$ das arestas de G. (*b*) Ache o grau de cada vértice e verifique o Teorema 8.1 para este grafo.

(*a*) Existem cinco vértices e $V(G) = [A, B, C, D, E]$. Existem sete pares de vértices $[x, y]$, onde o vértice x é conectado com o vértice y; portanto:

$$E(G) = [\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, E\}, \{C, D\}, \{C, E\}]$$

(*b*) O grau de um vértice é igual ao número de arestas aos quais ele pertence; por exemplo, $\deg(A) = 3$, já que A pertence a três arestas $[A, B]$ $[A, C]$ $[A, D]$. Analogamente,

$$\deg(B) = 3, \deg(C) = 4, \deg(D) = 2, \deg(E) = 2$$

A soma dos graus dos vértices é

$$3 + 3 + 4 + 2 + 2 = 14$$

que é igual a duas vezes o número de arestas.

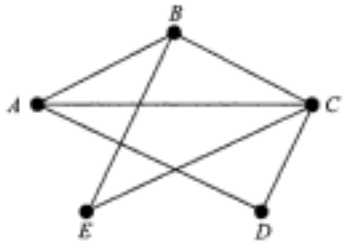


Fig. 8-31

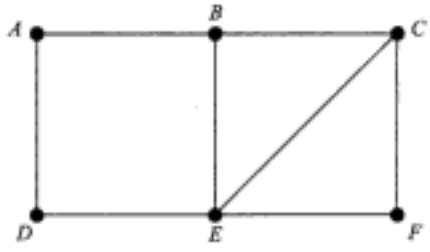


Fig. 8-32

8.2 Considere o grafo G da Figura 8-32. Ache: (*a*) todos os caminhos simples de A para F; (*b*) todas as trilhas de A para F; (*c*) $d(A,F)$; a distância de A para F; (*d*) diam(G); o diâmetro de G; (*e*) todos os ciclos que incluem o vértice A; (*f*) todos os ciclos em G.

(*a*) Um caminho simples de A para F é um caminho onde nenhum vértice, e logo nenhuma aresta, é repetida. Existem sete destes caminhos, quatro começando com as arestas $\{A, B\}$ e três começando com a aresta $\{A, D\}$:

$$(A, B, C, F), \quad (A, B, C, E, F), \quad (A, B, E, F), \quad (A, B, E, C, F);$$
$$(A, D, E, F), \quad (A, D, E, B, C, F), \quad (A, D, E, C, F)$$

(*b*) Uma trilha de A para F é um caminho tal que nenhuma aresta é repetida. Existem nove destas trilhas: os sete caminhos simples de (*a*) junto com

$$(A, D, E, B, C, E, F) \qquad \text{e} \qquad (A, D, E, C, B, E, F)$$

(*c*) Existe um caminho, por exemplo, (A, B, C, F), de A para F de comprimento 3, e não há nenhum caminho mais curto; portanto, $d(A, F) = 3$.

(*d*) A distância entre quaisquer dois vértices não é maior do que 3, e a distância de A para F é 3; portando, diam(G) = 3.

(*e*) Um ciclo é um caminho fechado em que nenhum vértice é repetido (exceto o primeiro e o último). Existem três ciclos que incluem o vértice A:

$$(A, B, E, D), \quad (A, B, C, E, D, A), \quad (A, B, C, F, E, D, A)$$

(*f*) Existem seis ciclos em G: os três em (*e*) e

$$(B, C, E, B), \quad (C, F, E, C), \quad (B, C, F, E, B)$$

8.3 Considere os multigrafos G da Figura 8-33. (*a*) Quais dentre eles são conexos? (*b*) Se um grafo não é conexo, ache suas componentes conexas. (*c*) Quais são acíclicos (sem ciclos)? (*c*) Quais não contêm laços? (*d*) Quais são grafos?

(*a*) Apenas (1) e (3) são conexos. (2) é desconexo; suas componentes conexas são $\{A, D, E\}$ e $\{B, C\}$. (4) é desconexo; suas componentes são $\{A, B, E\}$ e $\{C, D\}$.

(*b*) Apenas (1) e (4) são acíclicos. (2) tem o ciclo (A, D, E, A), e (3) tem o ciclo (A, B, E, A).

(*c*) Apenas (4) tem um laço, que é $\{B, B\}$.

(*d*) Apenas (1) e (2) são grafos. O multigrafo (3) tem as arestas múltiplas $\{A, E\}$ e $\{A, E\}$; e (4) tem tanto as arestas múltiplas $\{C, D\}$ e $\{C, D\}$ quanto o laço $\{B, B\}$.

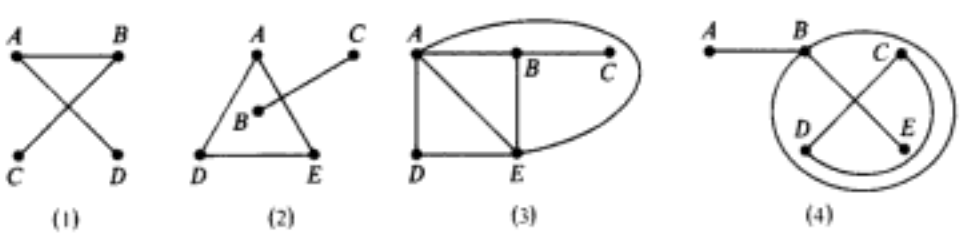


Fig. 8-33

8.4 Seja G o grafo da Figura 8-34(*a*). Ache: (*a*) todos os caminhos simples de A para C; (*b*) todos os ciclos; (*c*) o subgrafo H de G gerado por $V' = \{B, C, X, Y\}$; (*d*) $G - Y$; (*e*) todos os pontos de corte; (*f*) todas as conexões.

(*a*) Existem dois caminhos simples de A para C: (A, X, Y, C) e (A, X, B, Y, C).

(*b*) Existe um ciclo: (B, X, Y, B).

(*c*) Como representado na Figura 8-34(*b*), H consiste nos vértices V' e no conjunto E' de todas as arestas cujos extremos pertencem a V', isto é,

$$E' = [\{B, X\}, \{X, Y\}, \{B, Y\}, \{C, Y\}]$$

(*d*) Delete o vértice Y de G e todas as arestas que contêm Y para obter o grafo $G - Y$ da Figura 8-34(*c*). (Note que Y é um ponto de corte, uma vez que $G - Y$ é desconexo.)

(*e*) Os vértices A, X e Y são pontos de corte.

(*f*) Uma aresta e é uma conexão se $G - e$ é desconexo. Portanto, existem três conexões: $\{A, Z\}$, $\{A, X\}$ e $\{C, Y\}$.

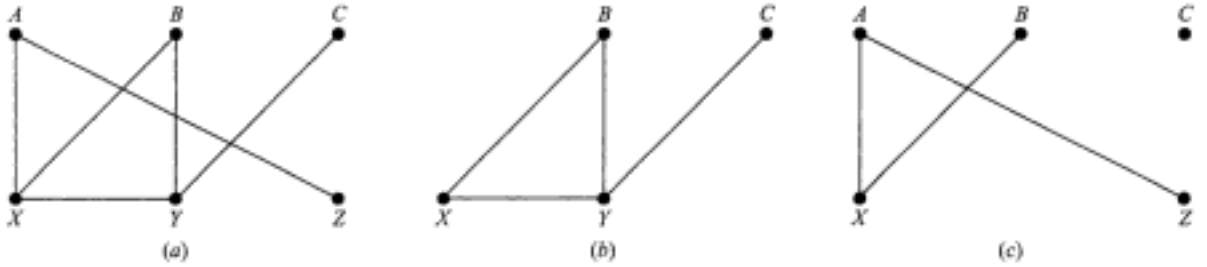


Fig. 8-34

8.5 Considere o grafo G da Figura 8-32. Ache os subgrafos obtidos quando cada vértice é deletado. G tem pontos de corte?

Quando deletamos um vértice de G, temos que deletar também todas as arestas que contêm o vértice. Os seis grafos obtidos quando se deleta cada um dos vértice de G estão na Figura 8-35. Todos os seis grafos são conexos. Portanto, nenhum vértice é um corte.

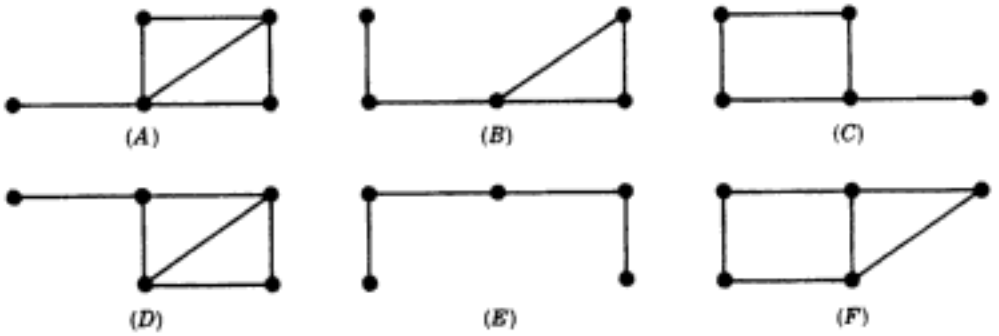


Fig. 8-35

8.6 Mostre que os seis grafos obtidos no Problema 8.5 são distintos, isto é, nenhum par é isomorfo. Mostre também que (*B*) e (*C*) são isomorfos.

Os graus dos cinco vértices de qualquer um dos grafos não podem ser igualados com os graus de outro grafo, exceto (*B*) e (*C*). Portanto, nenhum dos grafos é isomorfo a outro, exceto possivelmente (*B*) e (*C*).

Entretanto, se deletarmos os vértices de grau 3 em (*B*) e (*C*), obtemos subgrafos distintos. Portanto, (*B*) e (*C*) não são isomorfos; logo, os seis grafos são distintos. Porém, (*B*) e (*C*) são homeomorfos já que podem ser obtidos, respectivamente, dos grafos isomorfos da Figura 8-36 adicionando os vértices apropriados.

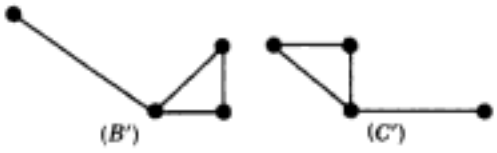


Fig. 8-36

Grafos Atravessáveis, Circuitos Eulerianos e Hamiltonianos

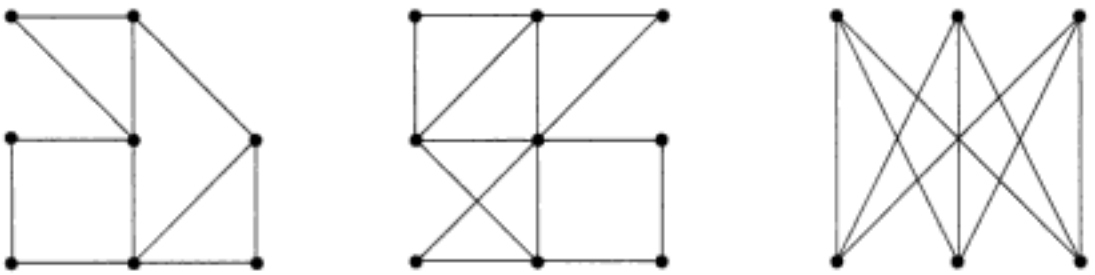
8.7 Considere cada grafo G da Figura 8-37. Quais deles são atravessáveis, isto é, têm caminhos de Euler? Quais são eulerianos, isto é, têm um circuito de Euler? Para aqueles que não têm, explique por quê.

G é atravessável (tem um caminho de Euler) apenas se 0 ou 2 vértices têm grau ímpar, e G é euleriano (tem um circuito de Euler) se todos os vértices têm grau par (Teorema 8.3).

(*a*) Atravessável, já que existem dois vértices ímpares. Os caminhos atravessáveis precisam começar em um dos vértices ímpares e terminar no outro.

(*b*) Atravessável, já que todos os vértices são pares. Portanto, G tem um circuito de Euler.

(*c*) Já que seis vértices têm grau par, G não é atravessável.



(*a*) (*b*) (*c*)

Fig. 8-37

8.8 Quais dos grafos G da Figura 8-37 têm um circuito hamiltoniano? Se não, por quê?

Os grafos (*a*) e (*c*) têm circuitos hamiltonianos. (O leitor deverá ser capaz de, facilmente, determinar algum.) Entretanto, o grafo (*b*) não tem circuito hamiltoniano, pois, se α é um circuito hamiltoniano, então α deve conectar o vértice intermediário com o vértice superior direito e depois seguir ao longo da linha inferior para o vértice inferior direito, depois ir verticalmente para o intermediário direito – mas então será forçado a visitar o vértice central antes de visitar os vértices restantes.

8.9 Prove o Teorema 8.3 (Euler): um grafo conexo finito G é euleriano se e somente se cada vértice tem grau par.

Suponha que G é euleriano e T é uma trilha euleriana fechada. Para cada vértice v de G, a trilha T chega em v e deixa v o mesmo número de vezes sem repetir arestas. Portanto, v tem grau par.

Suponha, conversamente, que cada vértice de G tem grau par. Costruímos uma trilha euleriana. Começamos com uma trilha T_1 e uma aresta e qualquer. Estendemos T_1 adicionando um vértice depois do outro. Se T_1 não é fechada em nenhum passo, digamos, T_1 começa em u mas termina em $v \neq u$; então, apenas um número ímpar de arestas incidentes em v aparece em T_1; portanto, podemos estender T_1 por outra aresta incidente em v. Logo, podemos continuar a estender T_1 até que T_1 retorne para o seu vértice inicial u, isto é, até que T_1 seja fechada. Se T_1 inclui todas as arestas de G, então T_1 é nossa trilha euleriana.

Suponha que T_1 não inclui todas as arestas de G. Considere o grafo H obtido pela deleção de todas as arestas em T_1 de G. H pode não ser conexo, mas cada vértice de H tem grau par, já que T_1 contém um número par de arestas incidentes em qualquer vértice. Como G é conexo, existe uma aresta e' de H que tem um extremo u' em T_1. Construímos uma trilha T_2 em H começando em u' e usando e'. Como todos os vértices de H têm grau par, podemos continuar a estender T_2 em H até que T_2 retorne para u', como representado na Figura 8-38. Claramente, podemos colocar T_1 e T_2 juntos para formar uma trilha fechada maior em G. Continuamos o processo até que todas as arestas de G sejam usadas. Finalmente obtemos uma trilha euleriana e, portanto, G é euleriano.

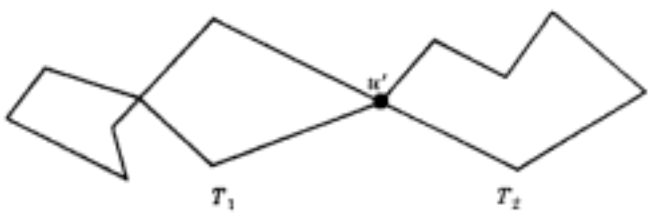
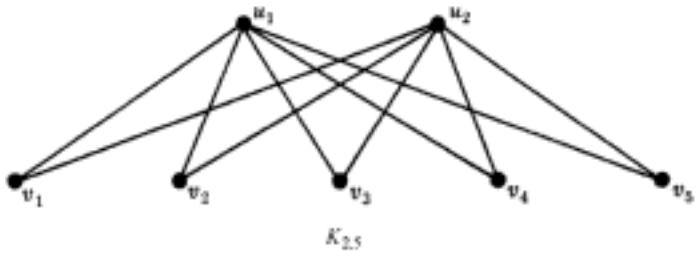


Fig. 8-38

Grafos Especiais

8.10 Desenhe o grafo $K_{2,5}$

$K_{2,5}$ consiste em sete vértices particionados em um conjunto M de dois vértices, digamos, u_1 e u_2, e um conjunto N de cinco vértices, digamos, $v_1, v_2, \ldots, v_5$, e todas as possíveis arestas de um vértice u_i para um vértice u_j. Portanto, existem 10 arestas. O grafo aparece na Figura 8-39.



$K_{2,5}$

Fig. 8-39

8.11 Quais grafos conexos podem ser regulares e biparticionados?

O grafo biparticionado $K_{m,n}$ é regular de grau m, já que cada vértice é conectado a m outros vértices e, portanto, tem grau m. Subgrafos de $K_{m,n}$ podem também ser regulares se forem deletadas m arestas disjuntas. Por exemplo, o subgrafo de $K_{4,4}$ mostrado na Figura 8-40 é 3-regular. Podemos continuar a deletar m arestas disjuntas e obter, a cada vez, um grafo regular com um grau a menos. Esses grafos podem ser desconexos, mas em qualquer caso suas componentes conexas têm as propriedades desejadas.

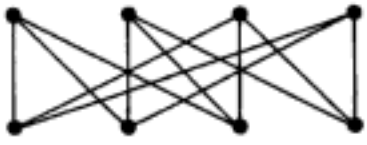


Fig. 8-40

Árvores e Árvores Geradoras

8.12 Desenhe todas as árvores com exatamente seis vértices.

Existem seis destas árvores que estão exibidas na Figura 8-41. A primeira árvore tem diâmetro 5, as duas seguintes, diâmetro 4, as duas seguintes, diâmetro 3, e a última, diâmetro 2. Qualquer outra árvore com seis nós é isomorfa a uma destas árvores.

Fig. 8-41

8.13 Ache todas as árvores geradoras do grafo G mostrado na Figura 8-42(a).

Existem seis destas árvores geradoras como mostrado na Figura 8-42(b). Cada árvore geradora deve ter $4 - 1 = 3$ arestas, uma vez que G tem quatro vértices. Logo, cada árvore pode ser obtida deletando-se duas das cinco arestas de G. Isto pode ser feito de 10 maneiras, exceto pelo fato de que duas das maneiras levam a grafos desconexos. Portanto, as oito árvores geradoras são todas as árvores geradoras de G.

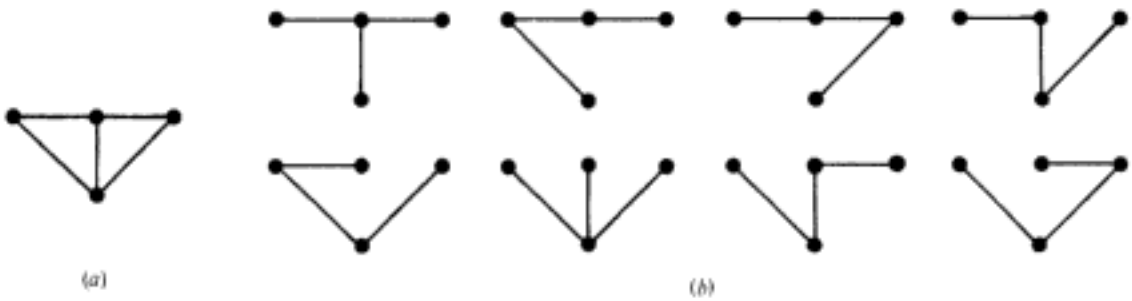


Fig. 8-42

8.14 Ache todas as árvores geradoras T para o grafo ponderado G da Figura 8-43(a).

Como G tem $n = 9$ vértices, T precisa ter $n - 1 = 8$ arestas. Aplique o Algoritmo 8.8A, isto é, delete seqüencialmente arestas de comprimento máximo sem desconectar o grafo, até que restem apenas $n - 1 = 8$ arestas. Como outra opção, aplique o Algoritmo 8.8B, isto é, iniciando com os nove vértices, adicione sucessivamente arestas com comprimento mínimo e sem formar ciclos, até que sejam adicionadas $m - 1 = 8$ arestas. Ambos os métodos formam uma árvore geradora mínima como a exibida na Figura 8-43(b).

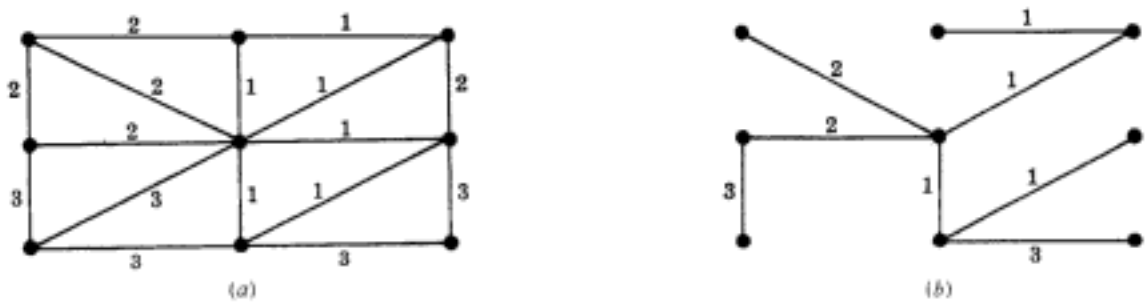


Fig. 8-43

8.15 Seja G um grafo com mais de um vértice. Prove que as seguintes afirmações são equivalentes: (i) G é uma árvore. (ii) Cada par de vértices está conectado por exatamente um caminho simples. (iii) G é conexo; mas $G - e$ é desconexo para qualquer aresta e de G. (iv) G é acíclico, mas se qualquer aresta é adicionada a G, o grafo resultante tem exatamente um ciclo.

(*i*) *implica* (*ii*). Sejam u e v dois vértices em G. Como G é árvore, G é conexo, de modo que existe pelo menos um caminho entre u e v. Pelo Problema 8.37, só pode existir um caminho simples entre u e v; caso contrário, G conteria um ciclo.

(*ii*) *implica* (*iii*). Suponha que deletemos uma aresta $e = \{u, v\}$ de G. Note que e é um caminho de u para v. Suponha que o grafo resultante $G - e$ tem um caminho P de u para v. Então, P e e são dois caminhos distintos de u para v, contradizendo a hipótese. Então não existe caminho entre u e v em $G - e$; logo, $G - e$ é desconexo.

(*iii*) *implica* (*iv*). Suponha que G contém um ciclo C que contém uma aresta $e = \{u, v\}$. Por hipótese, G é conexo, mas $G' = G - e$ é desconexo com u e v pertencendo a diferentes componentes de G' (Problema 8-41). Isso contradiz o fato de que u e v são conectados pelo caminho $P = C - e$ que está em G'. Portanto, G é acíclico. Agora, sejam x e y vértices de G, e seja H o grafo obtido pelo acréscimo da aresta $e = \{x, y\}$ a G. Como G é conexo, existe um caminho de x para y em G; portanto, $C = Pe$ forma um ciclo em H. Suponha que H contém um outro ciclo C'. Como G é acíclico, C' deve conter a aresta e, digamos, $C' = P'e$. Então, P e P' são dois caminhos simples em G de x para y. (Veja Figura 8-44.) Pelo Problema 8-37, G contém um ciclo, o que contradiz o fato de que G é acíclico. Portanto, H contém apenas um ciclo.

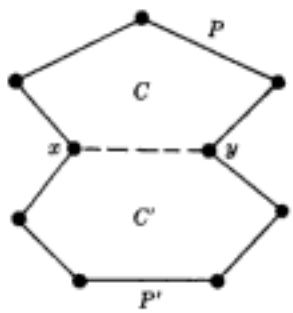


Fig. 8-43

(*iv*) *implica* (*i*). Como a adição de qualquer aresta $e = \{x, y\}$ a G produz um ciclo, os vértices precisam já estar conectados em G. Portanto, G é conexo e, por hipótese, G é acíclico; isto é, G é uma árvore.

8.16 Prove o Teorema 8.6: seja G um grafo finito com $n \geq 1$ vértices. As seguintes afirmativas são equivalentes. (i) G é uma árvore. (ii) G é acíclico e tem $n - 1$ arestas. (iii) G é conexo e tem $n - 1$ arestas.

A demonstração é por indução sobre n. O teorema certamente é verdade para o grafo que possui apenas um vértice e, portanto, nenhuma aresta. Isto é, o teorema vale para $n = 1$. Assumimos agora que $n > 1$ e que o teorema vale para grafos com menos do que n vértices.

(*i*) *implica* (*ii*). Suponha que G é uma árvore. Então G é acíclico, e precisamos mostrar apenas que G tem $n - 1$ arestas. Pelo Problema 8.38, G tem um vértice de grau 1. Deletando esse vértice e sua aresta, obtemos uma árvore T que tem $n - 1$ vértices. O teorema vale para T; portanto, T tem $n - 2$ arestas. Logo, G tem $n - 1$ arestas.

(*ii*) *implica* (*iii*). Suponha que G é acíclico e tem $n - 1$ arestas. Precisamos mostrar apenas que G é conexo. Suponha que G é desconexo e tem k componentes $T_1, \ldots, T_k$, que são árvores, uma vez que cada uma é conexa e acíclica. Digamos que T_i tem n_i vértices. Note que $n_i < n$. Portanto, o teorema vale para T_i, e logo T_i tem n_i arestas. Portanto,

$$n = n_1 + n_2 + \cdots + n_k$$

e

$$n - 1 = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n_1 + n_2 + \cdots + n_k - k = n - k$$

Assim, $k = 1$. Mas isso contradiz a hipótese de que G é desconexo e tem $k > 1$ componentes. Logo, G é conexo.

(*iii*) *implica* (*i*). Suponha que G é conexo e tem $n - 1$ arestas. Precisamos mostrar apenas que G é acíclico. Suponha que G tem um ciclo contendo uma aresta e. Deletando e, obtemos o grafo $H = G - e$, que também é conexo. Mas H tem n vértices e $n - 2$ arestas, e isto contradiz o Problema 8.39. Logo, G é acíclico e, portanto, é uma árvore.

Grafos Planares

8.17 Desenhe uma representação planar de cada grafo da Figura 8-45, se possível.

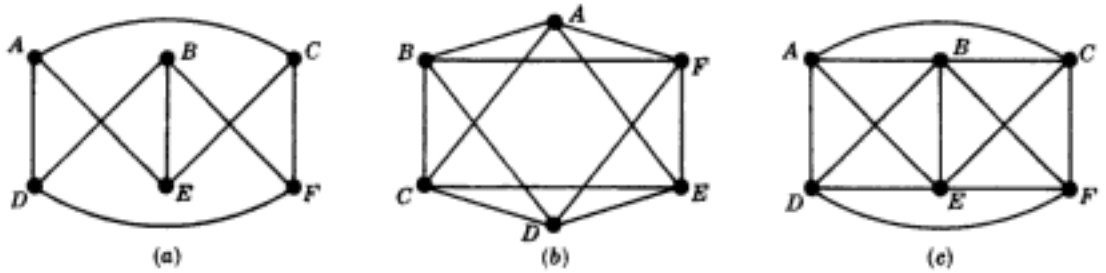


Fig. 8-45

(*a*) Redesenhando a posição dos vértices B e E, obtemos a representação planar do grafo, como na Figura 8-46(*a*).

(*b*) Este não é o grafo estrela K_5. Este tem uma representação planar como na Figura 8-46(*b*).

(*c*) Este grafo é não planar. O *utility graph* é um subgrafo como mostrado na Figura 8-46(*c*), onde redesenhamos as posições de C e F.

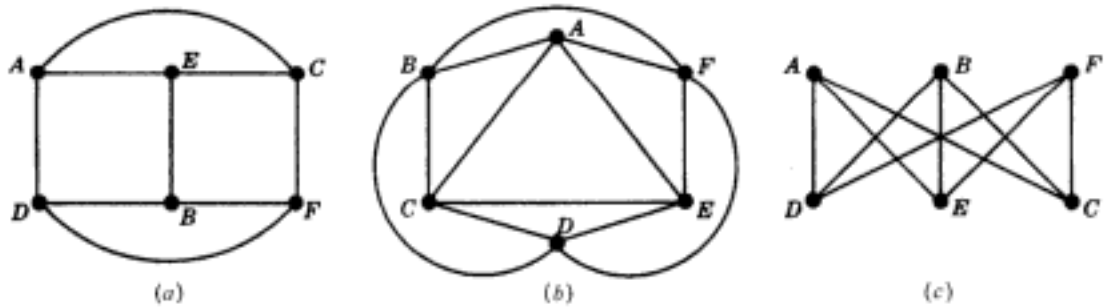


Fig. 8-46

8.18 Conte o número V de vértices, o número E de arestas e o número R de regiões de cada mapa na Figura 8-47 e verifique a fórmula de Euler. Ache também o grau da região externa.

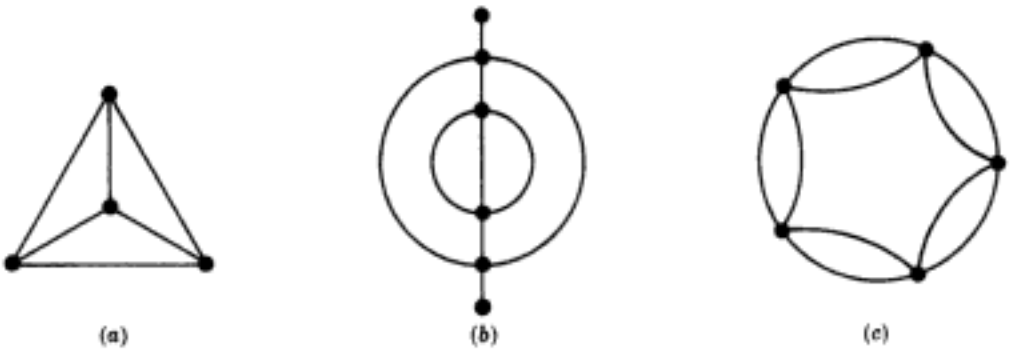


Fig. 8-47

(*a*) $V = 4, E = 6, R = 4$. Portanto, $V - E + R = 4 - 6 + 4 = 2$. Além disso, $d = 3$.

(*b*) $V = 6, E = 9, R = 5$. Portanto, $V - E + R = 6 - 9 + 5 = 2$. Aqui $d = 6$, já que duas arestas são contadas duas vezes.

(*c*) $V = 5, E = 10, R = 7$. Portanto, $V - E + R = 5 - 10 + 7 = 2$. Também $d = 5$.

8.19 Ache o menor número de cores necessárias para pintar cada mapa da Figura 8-47.

(*a*) $n = 4$; (*b*) $n = 3$; (*c*) são necessárias apenas duas cores, i. e., $n = 2$

8.20 Prove o Teorema 8.8 (Euler): $V - E + R = 2$.

Suponha que o mapa M consiste em um único vértice P como na Figura 8-48(*a*). Então, $V = 1, E = 0$ e $R = 1$. Logo, $V - E + R = 2$. Caso contrário, M pode ser montado a partir de um vértice isolado usando as seguintes duas construções:

(1) Acrescente um novo vértice Q_2 e conecte-o a um vértice existente Q_1 por uma aresta que não corte nenhuma aresta existente, como na Figura 8-48(*b*).

(2) Conecte dois vértices existentes Q_1 e Q_2 por uma aresta e que não cruze nenhuma aresta existente, como na Figura 8-48(*c*).

Nenhuma das operações muda o valor de $V - E + R$. Logo, M tem o mesmo valor para $V - E + R$ do que no mapa com um único vértice, isto é, $V - E + R = 2$. Logo, o teorema está provado.

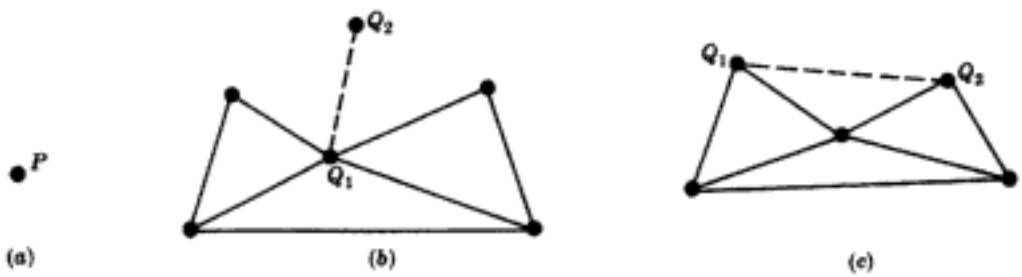


Fig. 8-48

8.21 Use o algoritmo de Welch-Powell para pintar o grafo da Figura 8-49, e ache o número cromático n do grafo.

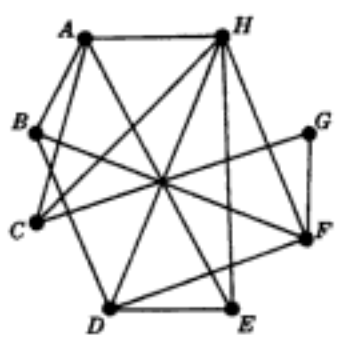


Fig. 8-49

Primeiramente ordene os vértices em ordem decrescente de grau para obter a seqüência

$$H, \quad A, \quad D, \quad F, \quad B, \quad C, \quad E, \quad G$$

Continuando seqüencialmente, usamos a primeira cor para pintar os vértices H, B e depois G. (Não podemos pintar A, D ou F com a primeira cor, pois cada um deles está conectado a H ou B.) Procedendo seqüencialmente com os vértices ainda não pintados, usamos a segunda cor para pintar os vértices A e D. Os vértices restantes, F, C e E, podem ser pintados com a terceira cor. Portanto, o número cromático n não pode ser maior do que 3. Entretanto, em qualquer coloração, os vértices H, D e E devem ser pintados com cores diferentes, pois estão conectados entre si. Logo, $n = 3$.

8.22 Prove o Teorema 8-11: as seguintes afirmativas são equivalentes para um grafo G: (i) G é 2-colorável. (ii) G é biparticionado. (iii) Todo ciclo de G tem comprimento par.

(*i*) *implica* (*ii*). Suponha que G é 2-colorável. Seja M o conjunto de vértices pintados com a primeira cor, e seja N o conjunto de vértices pintados com a segunda cor. Então M e N formam uma partição biparticionada dos vértices de G, já que vértices de M e N podem ser adjacentes um ao outro, pois têm a mesma cor.

(*ii*) *implica* (*iii*). Suponha que G é biparticionado e que M e N formam uma partição biparticionada dos vértices de G. Se um ciclo começar em um vértice u de, digamos, M, então ele irá para um vértice de N, e depois para um vértice de M, e então para N, e assim por diante. Portanto, quando o ciclo volta para u, deve ter comprimento par. Isto é, todo ciclo de G terá comprimento par.

(*iii*) *implica* (*i*). Finalmente suponha que todo ciclo de G tem comprimento par. Escolhemos um vértice em cada componente conexa e o pintamos com a primeira cor, por exemplo, vermelho. Depois, pintamos sucessivamente todos os vértices como a seguir: se um vértice é pintado de vermelho, então todos os vértices adjacentes a ele serão pintados com a segunda cor, por exemplo, azul. Se um vértice é pintado de azul, então todo vértice a ele adjacente será pintado de vermelho. Como todo ciclo tem comprimento par, dois vértices adjacentes não terão a mesma cor. Portanto, G é 2-colorável, e o teorema está provado.

8.23 Seja G um grafo planar conexo com pelo menos três vértices. Mostre que G tem pelo menos um vértice de grau 5 ou menos.

Seja p o número de vértices e q o número de arestas de G, e suponha que $\deg(u) \geq 6$ para cada vétice u de G. Mas $2q$ é igual à soma dos graus dos vértices de G (Teorema 8.1); portanto, $2q \geq 6q$. Logo,

$$q \geq 3p > 3p - 6$$

Isso contradiz o Teorema 8.9. Conseqüentemente, algum vértice de G tem grau menor ou igual a 5.

8.24 Prove o Teorema 8.12: um grafo planar G é 5-colorável.

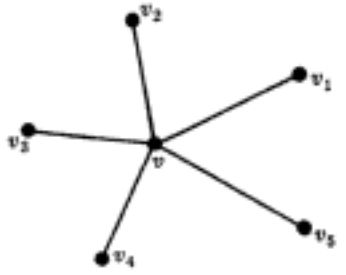


Fig. 8-50

A prova será feita por indução sobre o número p dos vértices de G. Se $p \leq 5$, o teorema obviamente vale. Suponha que $p > 5$ e que o teorema vale para grafos com menos do que p vértices. Pelo problema anterior, G tem um vértice v tal que $\deg(v) \leq 5$. Por indução, o subgrafo $G - v$ é 5-colorável. Suponha que seja feita alguma coloração deste tipo. Se os vértices adjacentes a v usam menos do que cinco cores, então simplesmente pinte v com uma das cores restantes para obter uma 5-coloração de G. Ainda temos de tratar do caso em que os cinco vértices adjacentes a v estão pintados com cores diferentes. Suponha que os vértices, movendo-se no sentido anti-horário em torno de v, $v_1, \ldots, v_5$, estão pintados, respectivamente, com as cores, $c_1, \ldots, c_5$. (Veja a Figura 8-50.)

Considere agora o subgrafo H de G gerado pelos vértices pintados por c_1 e c_3. Note que H inclui v_1 e v_3. Se v_1 e v_3 pertencem a componentes distintas de H, então podemos trocar as cores c_1 e c_3 na componente que contém v_1 sem destruir a coloração de $G - v$. Então, v_1 e v_3 são pintados por c_3, c_3 pode ser escolhido para pintar v, e temos uma 5-coloração de G. Por outro lado, suponha que v_1 e v_3 estão na mesma componente H. Então existe um caminho P de v_1 para v_3 cujos vértices são pintados com c_1 ou c_3. O caminho P, juntamente com as arestas $\{v, v_1\}$ e $\{v, v_3\}$, forma um ciclo C que envolve v_2 ou v_4. Considere agora o subgrafo K gerado pelos vértices pintados com c_2 ou c_4. Como C envolve v_2 ou v_4, mas não ambos, os vértices v_2 e v_4 pertencem a diferentes componentes de K. Portanto, podemos trocar as cores c_2 e c_4 na componente contendo v_2 sem destruir a coloração de $G - v$. Então, v_2 e v_4 são pintados por c_4, e podemos escolher c_2 para pintar v e obter uma 5-coloração de G. Portanto, G é 5-colorável, e o teorema está provado.

Representação Seqüencial de Grafos

8.25 Ache a matriz de adjacências $A = [a_{ij}]$ de cada grafo G da Figura 8-51.

Faça $a_{ij} = n$ se existirem n arestas $\{v_i, v_j\}$ e $a_{ij} = 0$, caso contrário. Portanto,

$$(a)\quad A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \qquad (b)\quad A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

(Como (a) não há arestas múltiplas nem laços, os elementos de A são 0 ou 1, e a diagonal apresenta 0.)

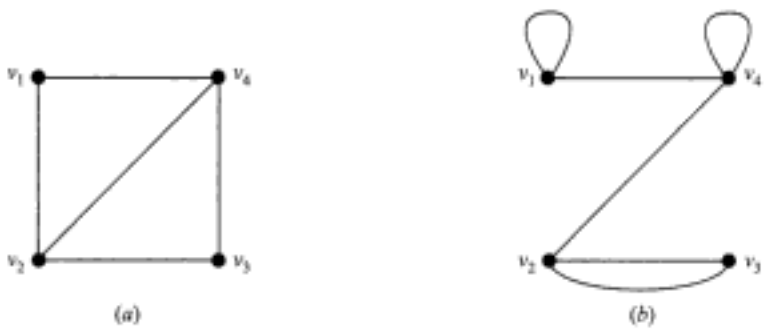


Fig. 8-51

8.26 Desenhe o grafo G que corresponde a cada uma das matrizes de adjacência seguintes:

$$(a)\quad A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}; \qquad (b)\quad A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

(a) Como A é uma matriz quadrada 5-dimensional, G tem cinco vértices, a saber, $v_1, v_2, \ldots, v_5$. Desenhe uma aresta de v_i para v_j quando $a_{ij} = 1$. O grafo aparece na Figura 8-52(a).

(*b*) Como A é uma matriz quadrada 4-dimensional, G tem quatro vértices, a saber, $v_1, \ldots, v_4$. Desenhe n arestas de v_i para v_j quando $a_{ij} = n$. Desenhe também n laços em v_i quando $a_{ii} = n$. O grafo aparece na Figura 8-52(*b*).

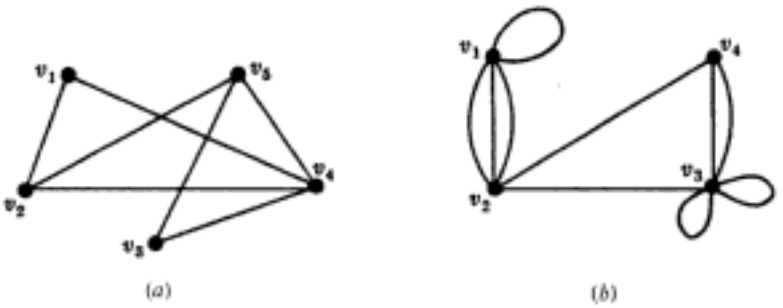


Fig. 8-52

8.27 Considere o grafo ponderado G da Figura 8-53. Suponha que os vértices estejam armazenados no *array* DATA como a seguir:

$$\text{DATA: } A, B, C, X, Y$$

Ache a matriz de pesos $W = (w_{ij})$ do grafo G.

Os vértices são numerados de acordo com a forma em que estão armazenados no *array* DATA. Isto é, $v_1 = A$, $v_2 = B, \ldots, v_5 = Y$. Então, faça $w_{ij} = w$, onde w é o peso da aresta de v_i para v_j. Portanto,

$$W = \begin{bmatrix} 0 & 6 & 0 & 4 & 1 \\ 6 & 0 & 5 & 0 & 8 \\ 0 & 5 & 0 & 0 & 2 \\ 4 & 0 & 0 & 0 & 3 \\ 1 & 8 & 2 & 3 & 0 \end{bmatrix}$$

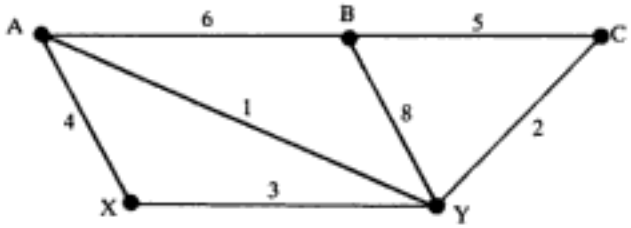


Fig. 8-53

Representação Ligada de Grafos

8.28 Um grafo G, com vértices $A, B, \ldots, F$ é armazenado na memória usando uma representação ligada com um arquivo de vértices e um arquivo de arestas como na Figura 8-54.

Arquivo de vértices

		1	2	3	4	5	6	7	8
START 4	VÉRTICE	*B*		*F*	*D*	*A*		*C*	*E*
	PROX-V	3		5	1	8		0	7
	PTR	9		4	7	6		5	12

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ADJ	4	4	1	8	8	1	5	3	5	8	4	7		
PROX	8	0	10	0	0	2	3	0	11	0	0	1		

Fig. 8-54

(*a*) Liste os vértices na ordem em que eles aparecem na memória.

(*b*) Ache a lista de adjacências adj (v) de cada vértice v de G.

(*a*) Como START = 4, a lista começa com o vértice D. PROX– V manda ir para 1(B), então 3(F), então 5(A), depois 8(E), e então 7(C); isto é:

$$D, \quad B, \quad F, \quad A, \quad E, \quad C$$

(*b*) Aqui, adj (D) = [5(*A*), 1(*B*), 8(*E*)]. Especificamente, PTR[4(D)] = 7 e ADJ [7] = 5(A) nos diz que adj(D) começa com A. Depois, PROX [7] = 3 e ADJ[3] = 1(B) nos diz que B é o próximo vértice em adj(D). Depois, PROX [3] = 10 e ADJ[10] = 8(E) nos diz que E é o próximo vértice em adj(D). Entretanto, PROX [10] = 0 nos diz que não existem mais vizinhanças de D. Analogamente,

$$\text{adj}\,(B) = [A, D], \quad \text{adj}\,(F) = [E], \quad \text{adj}\,(A) = [B, D], \quad \text{adj}\,(E) = [C, D, F], \quad \text{adj}\,(C) = [E]$$

Em outras palavras, a estrutura de adjacências de G é a seguinte:

$$G = [A{:}B, D; \quad B{:}A, D; \quad C{:}E; \quad D{:}A, B, E; \quad E{:}C, D, F; \quad F{:}E]$$

8.29 Desenhe o diagrama do grafo G cuja representação ligada aparece na Figura 8-54.

Use a lista de vértices obtida no Problema 8-28(*a*) e a lista de adjacências obtida no Problema 8.28(*b*) para desenhar o grafo de G como na Figura 8-55.

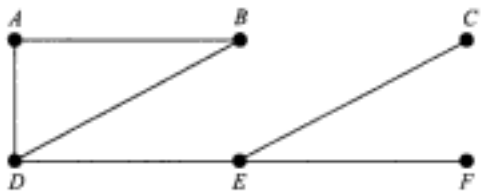


Fig. 8-55

8.30 Determine a estrutura de adjacências do grafo G em: (*a*) Figura 8-31; (*b*) Figura 8-32.

A estrutura de adjacências de um grafo G consiste na lista de adjacências dos vértices em que usamos dois-pontos ":" para separar um vértice e sua lista de adjacências e um ponto-e-vírgula ";" para separar listas diferentes. Logo:

(*a*) $G = [A{:}B, C, D; \quad B{:}A, C, E; \quad C{:}A, B, D, E; \quad D{:}A, C; \quad E{:}B, C]$

(*b*) $G = [A{:}B, D; \quad B{:}A, C, E; \quad C{:}B, E, F; \quad D{:}A, E; \quad E{:}B, C, D, F; \quad F{:}C, E]$

Algoritmos em Grafos

8.31 Considere o grafo G da Figura 8.56.

(*a*) Ache a estrutura de adjacências de G.

(*b*) Ache a ordem em que os vértices de G são processados usando um algoritmo de busca em profundidade iniciando no vértice A.

(*a*) Liste as vizinhanças de cada vértice como a seguir:

$$G = [A{:}B, C, D; \quad B{:}A, E; \quad C{:}A; \quad D{:}A, F; \quad E{:}B, F, H; \quad F{:}D, E, G; \quad G{:}F, H; \quad H{:}E, G]$$

(*b*) Durante o algoritmo de busca em profundidade, o primeiro vértice N em PILHA é processado, e as vizinhanças de N (que não foram previamente processadas) são inseridas em PILHA. Inicialmente, o vértice inicial A é inserido na PILHA. A tabela seguinte mostra a seqüência da lista de espera em PILHA e os vértices sendo processados:

Vértices		*A*	*B*	*E*	*F*	*D*	*G*	*H*	*C*
PILHA	*A*	*BCD*	*ECD*	*FHCD*	*DGHCD*	*GHC*	*HHC*	*C*	

Em outras palavras, os vértices são processados na ordem *A*, *B*, *E*, *F*, *D*, *G*, *H*, *C*.

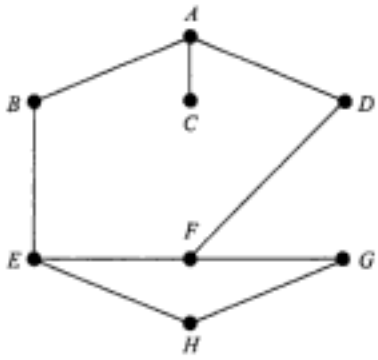


Fig. 8-56

8.32 Ache a ordem em que os vértices do grafo *G* da Figura 8-56 são processados usando o algoritmo de busca em largura, começando no vértice *A*.

Durante o algoritmo BFS, o primeiro vértice *N* na FILA é processado, e as vizinhanças de *N* (que não apareceram previamente) são então adicionadas em FILA. Inicialmente, o vértice inicial *A* é atribuído à FILA. A tabela seguinte mostra a seqüência da lista de espera em PILHA e os vértices sendo processados:

Vértices		*A*	*B*	*C*	*D*	*E*	*F*	*H*	*G*
FILA	*A*	*BCD*	*CDE*	*DE*	*EF*	*FH*	*HG*	*G*	

Em outras palavras, os vértices são processados na ordem *A*, *B*, *C*, *D*, *E*, *F*, *H*, *G*.

Problemas Complementares

8.33 Considere o grafo da Figura 8-57. Ache: (*a*) o grau de cada vértice (verifique o Teorema 8.1); (*b*) todos os caminhos simples de *A* para *G*; (*c*) todas as trilhas (arestas distintas) de *B* para *C*; (*d*) *d*(*A*, *C*), a distância entre *A* e *C*; (*e*) diam(*G*), o diâmetro de *G*.

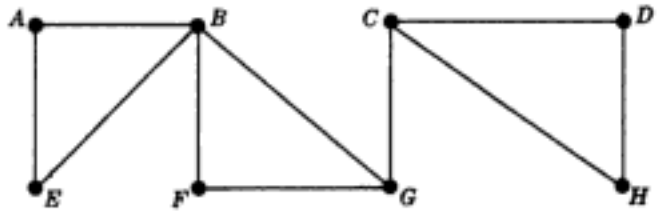


Fig. 8-57

8.34 Considere o grafo da Figura 8-57. Ache: (*a*) todos os ciclos, se houver; (*b*) todos os pontos de corte, se houver; (*c*) todas as conexões, se houver.

8.35 Considere o grafo da Figura 8.57. Ache o subgrafo $H(V', E')$ gerado por: (*a*) $V' = \{B, C, D, E, F\}$; (*b*) $V' = \{A, C, E, G, H\}$; (*c*) $V' = \{B, D, E, H\}$; (*d*) $V' = \{C, F, G, H\}$.
Quais deles são isomorfos e quais são homeomorfos?

8.36 Considere os multigrafos *G* da Figura 8-58. (*a*) Quais deles são conexos? Se não forem, ache o número de componentes conexas. (*b*) Quais deles são acíclicos (sem ciclos)? Se não forem, ache o número de ciclos. (*c*) Quais não contêm laços? (*d*) Quais são grafos (simples)?

Fig. 8-58

8.37 Suponha que um grafo G contém dois caminhos distintos de um vértice u para um vértice G. Mostre que G tem um ciclo.

8.38 Suponha que G é um grafo finito sem ciclos com pelo menos uma aresta. Mostre que G tem pelo menos dois vértices de grau 1.

8.39 Mostre que um grafo conexo G com n vértices deve ter pelo menos $n - 1$ arestas.

8.40 Ache o número de grafos conexos com quatro vértices (desenhe-os).

8.41 Seja G um grafo conexo. Prove:

(*a*) Se G contém um ciclo C que contém uma aresta e, então $G - e$ é conexo.

(*b*) Se $e = \{u, v\}$ é uma aresta tal que $G - e$ é desconexo, então u e v pertencem a componentes conexas distintas de $G - e$.

8.42 Considere os dois passos seguintes em um grafo G: (1) Delete uma aresta. (2) Delete um vértice e todas as arestas contendo aquele vértice. Mostre que todo subgrafo H do grafo finito G pode ser obtido por uma seqüência desses dois passos.

Grafos Atravessáveis e Circuitos Eulerianos e Hamiltonianos

8.43 Considere o grafo G da Figura 8-59. Ache um caminho de Euler (atravessável) ou um circuito euleriano, se existirem. Se não existir, por que não?

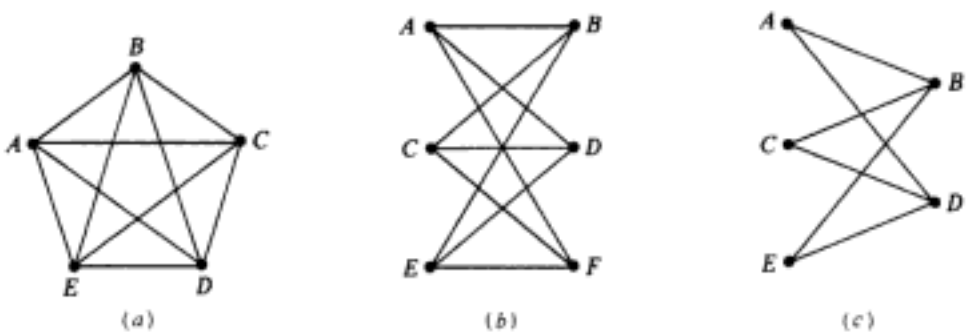


Fig. 8-59

8.44 Considere cada grafo G na Figura 8-59. Ache um caminho hamiltoniano ou um circuito hamiltoniano, se existirem. Se não existir, por que não?

8.45 Ache o número de circuitos hamiltonianos no grafo da Figura 8-59(*a*).

8.46 Suponha que G e G^* são grafos homeomorfos. Mostre que G é atravessável (euleriano) se e somente se G^* é atravessável (euleriano).

Grafos Especiais

8.47 Desenhe o grafo 3-regular com oito vértices.

8.48 Desenhe dois grafos 3-regulares com nove vértices.

8.49 Considere o grafo completo K_n.

(*a*) Ache o número m de arestas em K_n.

(*b*) Ache o grau de cada vértice em K_n.

(*c*) Ache os valores de n para os quais K_n é atravessável.

(*d*) Ache os valores de n para os quais K_n é regular.

8.50 Considere o grafo biparticionado $K_{m,n}$.

(*a*) Ache o diâmetro de $K_{m,n}$.

(*b*) Ache os $K_{m,n}$ que são atravessáveis.

(*c*) Quais dos grafos $K_{m,n}$ são isomorfos e quais são homeomorfos?

Árvores

8.51 Desenhe todas as árvores com quatro ou menos vértices.

8.52 Ache o número de árvores com sete vértices.

8.53 Ache o número de árvores geradoras da Figura 8-60.

8.54 Ache o peso da árvore geradora mínima da Figura 8-61.

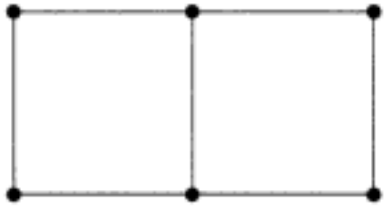


Fig. 8-60

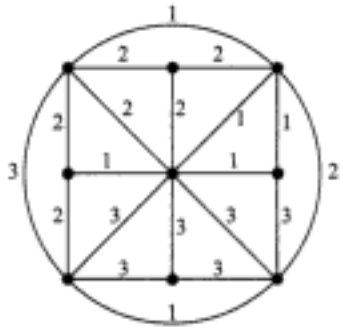


Fig. 8-61

8.55 Mostre que qualquer árvore é um grafo biparticionado.

8.56 Quais grafos completos biparticionados são árvores?

Grafos Planares, Mapas e Coloração

8.57 Desenhe a representação planar de cada grafo G da Figura 8-62, se possível. Caso contrário, mostre que existe um subgrafo homeomorfo a K_5 ou $K_{3,3}$.

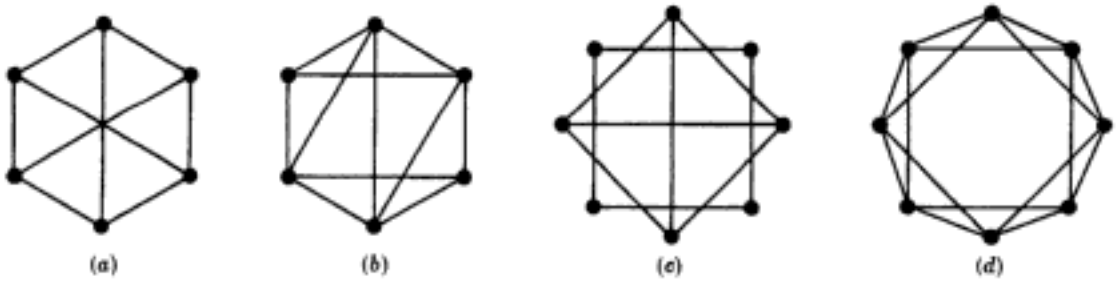


Fig. 8-62

8.58 Para o mapa da Figura 8-63, ache o grau de cada região e verifique que a soma dos graus das regiões é igual a duas vezes o número de arestas.

Fig. 8-63

8.59 Conte o número V de vértices, o número E de arestas e o número R de regiões de cada mapa da Figura 8-64 e verifique a fórmula de Euler.

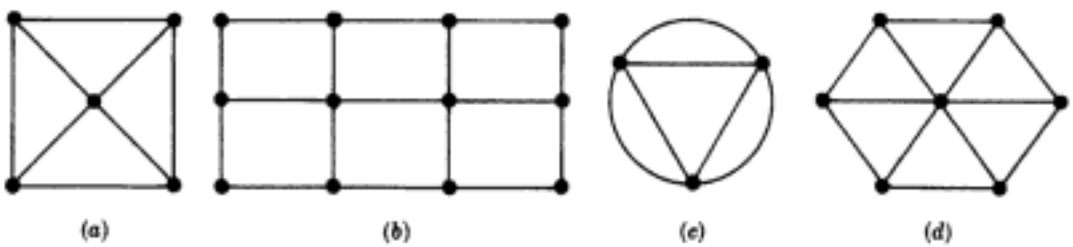


Fig. 8-64

8.60 Ache o menor número de cores necessárias para pintar as regiões de cada mapa da Figura 8-64.

8.61 Desenhe o mapa dual a cada mapa da Figura 8-64.

8.62 Use o algoritmo de Welch-Powell para pintar cada grafo da Figura 8-65. Ache o número cromático n do grafo.

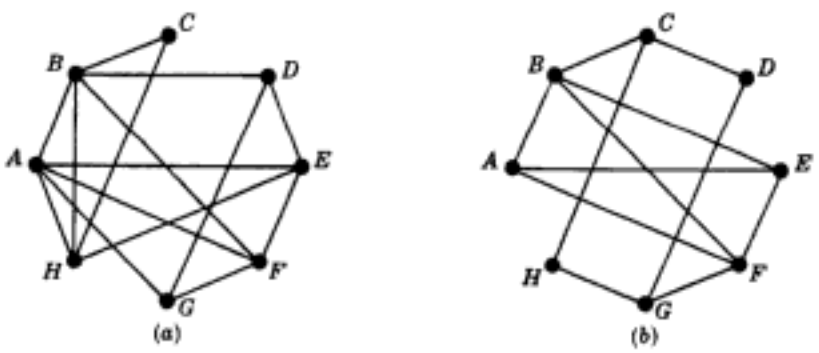


Fig. 8-65

Representação Sequencial de Grafos

8.63 Ache a matriz de adjacências A de cada grafo da Figura 8-66.

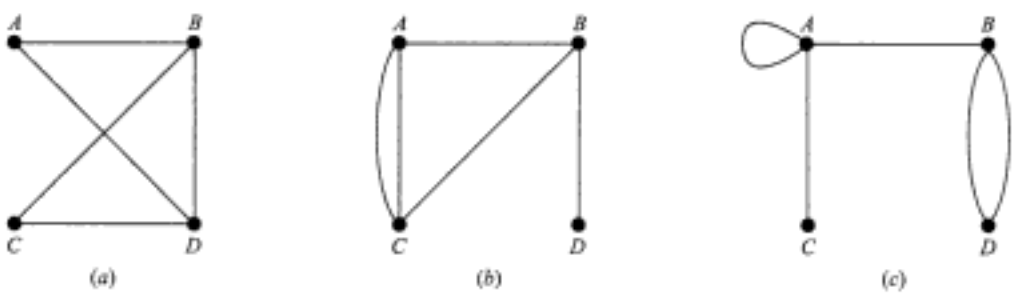


Fig. 8-66

8.64 Ache o multigrafo G correspondente a cada uma das matrizes de adjacências:

$$(a)\quad A=\begin{bmatrix}0&2&0&1\\2&1&1&1\\0&1&0&1\\1&1&1&0\end{bmatrix};\qquad (b)\quad A=\begin{bmatrix}1&1&1&2\\1&0&0&0\\1&0&0&2\\2&0&2&2\end{bmatrix}$$

8.65 Suponha que o grafo G é biparticionado. Mostre que os vértices de G podem ser ordenados de tal forma que a sua matriz de adjacências A tem a forma:

$$A=\begin{bmatrix}0&B\\C&0\end{bmatrix}$$

Representação Ligada de Grafos

8.66 Suponha que um grafo G é armazenado na memória como na Figura 8-67.

(*a*) Liste os vértices na ordem em que aparecem na memória.

(*b*) Ache a estrutura de adjacências de G, isto é, ache a lista de adjacências adj(v) de cada vértice v de G.

Arquivo de vértices

		1	2	3	4	5	6	7	8
START 7	VÉRTICE	*C*		*F*	*E*	*A*		*B*	*D*
	PROX-V	0		5	1	8		3	4
	PTR	2		11	6	12		4	1

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12
ADJ	7	7	4	5		7	1		8	3	1	7
PROX	0	10	0	7		0	9		3	0	0	0

Fig. 8-67

8.67 Exiba a estrutura de adjacências de cada grafo G da Figura 8-59.

8.68 A Figura 8-68 mostra um grafo G representando seis cidades $A, B, \ldots F$, conectadas por sete rodovias numeradas, 22, 33,..., 88. Mostre como G pode ser mantido na memória usando uma representação ligada com *arrays* ordenados para as cidades e as rodovias numeradas. (Note que VÉRTICES é um *array* ordenado e, logo, o campo PROX-V não é necessário.

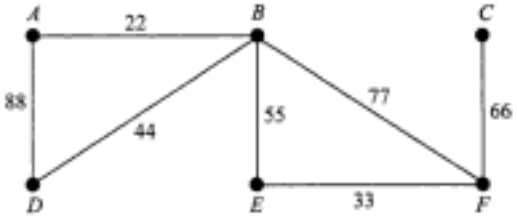


Fig. 8-68

Algoritmos para Grafos

8.69 Considere o grafo G da Figura 8-57.

Ache (*a*) a estrutura de adjacências de G e (*b*) a ordem em que os vértices de G são processados usando um algoritmo tipo DFS (busca em profundidade) começando em: (i) vértice C; (ii) vértice B.

8.70 Ache a ordem em que os vértices do grafo G da Figura 8-57 são processados usando um algoritmo do tipo BFS (busca em largura) começando em: (i) vértice C; (ii) vértice B.

Respostas dos Problemas Complementares

8.33 (*a*) 2, 4, 3, 2, 2, 2, 3, 2; (*b*) *ABG*, *ABFG*, *AEBG*, *AEBFG*; (*c*) *BGC*, *BFGC*, *BAEBGC*, *BAEBFGC*; (*d*) 3; (*e*) 4.

8.34 (*a*) *ABEA*, *BFGB*, *CDHC*; (*b*) *B*, *C*, *G*; (*c*) apenas $\{C, G\}$.

8.35 (*a*) $E' = \{BE, BF, CD\}$; (*b*) $E' = \{AE, FG, GC\}$; (*c*) $E' = \{BE, DH\}$; (*d*) $E' = \{FG, GC, CH\}$.
Além disso, (*a*) e (*b*) são isomorfos, e (*a*), (*b*) e (*c*) são homeomorfos.

8.36 (*a*) (iii) é conexo, (i) e (ii) têm duas componentes conexas; (*b*) nenhum, (i) 1, (ii) 2, (iii) 1; (*c*) (i) e (iii); (*d*) (iii).

8.38 *Sugestão*: considere um caminho maximal simples α, e mostre que seus extremos têm grau 1.

8.40 Existem cinco, como mostra a Figura 8-69.

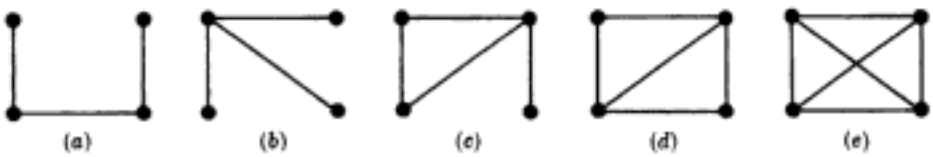


Fig. 8-69

8.42 Primeiramente delete todas as arestas de *G* que não estão em *H*; depois delete todos os vértices de *G* que não estão em *H*.

8.43 (*a*) Euleriano, uma vez que todos os vértices são pares: *ABCDEACEBDA*. (*b*) Nenhum, pois quatro vértices são ímpares. (*c*) Caminho de Euler começando em *D* e terminando em *D* (ou vice-versa): *BADCBED*.

8.44 (*a*) *ABCDEA*; (*b*) *ABCDEFA*; (*c*) nenhum, uma vez que *B* ou *D* precisam ser visitados duas vezes em qualquer caminho fechado incluindo todos os vértices.

8.45 $(5-1)!/2 = 12$.

8.46 *Sugestão*: adicionar um vértice pela divisão de uma aresta não muda o grau do vértice original e apenas adiciona um vértice de grau par.

8.47 Os dois grafos regulares da Figura 8-70 não são isomorfos já que *B* tem um 5-ciclo, mas (*a*) não tem.

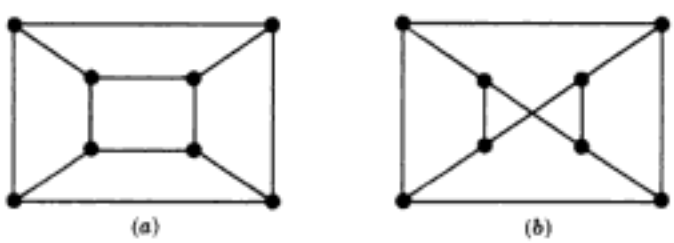


Fig. 8-70

8.48 Nenhum. A soma dos graus de qualquer grafo *r*-regular com *s* vértices é igual a *rs* e deve ser par.

8.49 (*a*) $m = C(n, 2) = n(n-1)/2$; (*b*) $n-1$; (*c*) $n = 2$ e n é ímpar; (*d*) qualquer n.

8.50 (*a*) $\text{diam}(K_{1,1}) = 1$; todos os outros têm diâmetro 2.

(*b*) $K_{1,1}$, $K_{1,2}$ e todo $K_{m,n}$, onde m e n são pares.

(*c*) Não existe isomorfismo; apenas $K_{1,1}$ e $K_{1,2}$ são homeomorfos.

8.51 Existem oito destas árvores, como mostrado na Figura 8-71. O grafo com um vértice e nenhuma aresta é dito a *árvore trivial*.

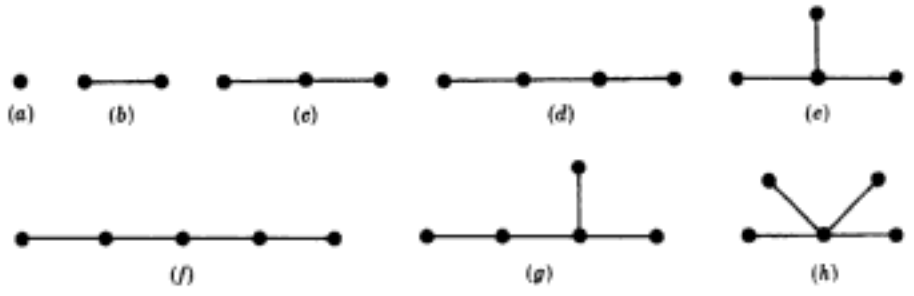


Fig. 8-71

8.52 10.

8.53 15.

8.54 $1+1+1+1+1+2+2+3=12$.

8.56 $m=1$.

8.57 Apenas (*a*) é não planar, e $K_{3,3}$ é subgrafo.

8.58 A região externa tem grau 8, e as outras duas regiões têm grau 5.

8.59 (*a*) 5, 8, 5; (*b*) 12, 17, 7; (*c*) 3, 6, 5; (*d*) 7, 12, 7.

8.60 (*a*) 3; (*b*) 3; (*c*) 2; (*d*) 3.

8.61 Veja a Figura 8-72.

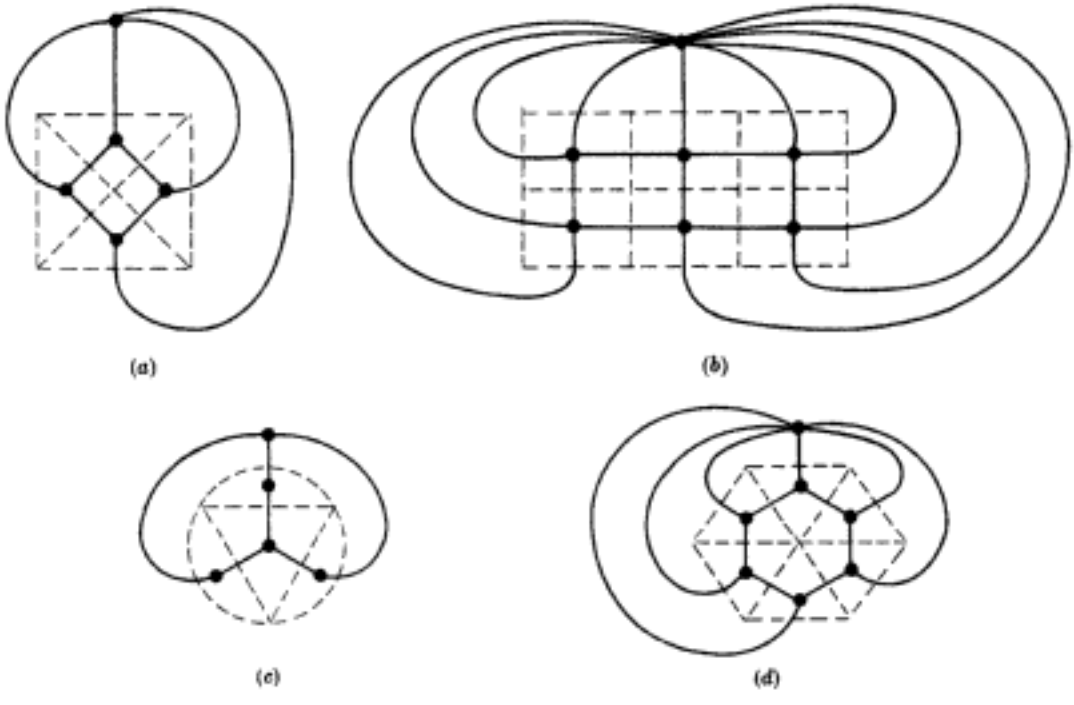


Fig. 8-72

8.62 (*a*) $n=3$; (*b*) $n=4$.

8.63 (*a*) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$; (*b*) $\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$; (*c*) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix}$.

8.64 Veja a Figura 8-73.

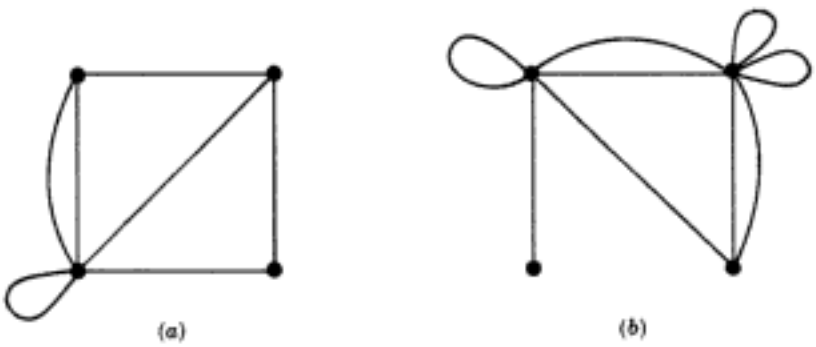


Fig. 8-73

8.65 Sejam M e N os dois conjuntos disjuntos de vértices que determinam o grafo biparticionado G. Ordene primeiramente os vértices em M e, depois, os que estiverem em N.

8.66 (*a*) B, F, A, D, E, C.
(*b*) $G = [A{:}B;\quad B{:}A, C, D, E;\quad C{:}F;\quad D{:}B;\quad E{:}B;\quad F{:}C]$.

8.67 (*a*) Cada vértice é adjacente aos outros quatro vértices.
(*b*) $G = [A{:}B, D, F;\quad B{:}A, C, E;\quad C{:}B, D, F;\quad D{:}A, C, E;\quad E{:}B, D, F;\quad F{:}A, C, E]$.
(*c*) $G = [A{:}B, D;\quad B{:}A, C, E;\quad C{:}B, D;\quad D{:}A, C, E;\quad E{:}B, D]$.

8.68 Veja a Figura 8-74.

Arquivo de vértices

	1	2	3	4	5	6	7	8
VÉRTICE	*A*	*B*	*C*	*D*	*E*	*F*		
PTR	1	2	9	14	8	12		

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
NÚMERO	22	22	33	33	44	44	55	55	66	66	77	77	88	88	
ADJ	2	1	6	5	4	2	5	2	6	3	6	2	4	1	
PROX	13	5	0	0	7	0	11	3	0	4	0	10	0	6	

Fig. 8-74

8.69 (*a*) $G = [A{:}B, E;\quad B{:}A, E, F, G;\quad C{:}D, G, H;\quad D{:}C, H;\quad E{:}A, B;\quad F{:}B, G;\quad G{:}B, C, F;\quad H{:}C, D]$.
(*b*) (i) C, D, H, G, B, A, E, F; (ii) B, A, E, F, G, C, D, H.

8.70 (*a*) C, D, G, H, B, F, A, E; (*b*) B, A, E, F, G, C, D, H.

Capítulo 9

Grafos Orientados

9.1 INTRODUÇÃO

Grafos orientados são grafos nos quais as arestas são direcionadas. Tais grafos têm utilidade freqüente em vários sistemas dinâmicos tais como computadores ou sistemas de fluxo. Entretanto, a adição dessa característica torna mais difícil a determinação de certas propriedades do grafo. Isto é, processar tais grafos pode ser semelhante a dirigir em uma cidade com muitas ruas de mão única.

Grafos orientados já foram tratados no Capítulo 3, na parte de relações. Pode-se encarar certos grafos orientados como relações binárias. Por esta razão, alguns textos discutem grafos orientados no contexto de relações. Na verdade, apresentaremos aqui um algoritmo eficiente para determinar o fecho transitivo de uma relação.

Este capítulo apresenta as definições e propriedades básicas de grafos orientados. Muitas das definições serão semelhante àquelas do capítulo precedente sobre grafos (não orientados). Entretanto, por razões pedagógicas, este capítulo é fundamentalmente independente do anterior.

9.2 GRAFOS ORIENTADOS

Um *grafo orientado G*, ou um *dígrafo*[†], consiste em:

(i) um conjunto $V = V(G)$ cujos elementos são chamados de *vértices*, *nós* ou *pontos*;
(ii) um conjunto E de pares *ordenados* de vértices (u, v), chamados de *arcos* ou *arestas orientadas* ou simplesmente *arestas*.

Escreveremos $G(V, E)$ quando quisermos enfatizar as duas partes de G. Também escreveremos $V(G)$ e $E(G)$ para denotar, respectivamente, o conjunto de vértices e o conjunto de arestas de um grafo G. (Quando não for explicitado, o contexto normalmente determina se um grafo G é orientado ou não.)

Suponha que $e = (u, v)$ é uma aresta orientada em um dígrafo G. Usamos a seguinte terminologia:

(*a*) e inicia em u e termina em v.
(*b*) u é a origem ou ponto inicial de e, e v é o destino ou ponto final de e.
(*c*) v é um sucessor de u.
(*d*) u é adjacente para v, e v é adjacente de u.

Se $u = v$, então e é dito um *laço*.

[†] N. de T. Em inglês, *directed graph*.

O conjunto de todos os sucessores de um vértice u é importante; ele é formalmente denotado e definido por:

$$\text{suc}\ (u) = \{v \in V\text{: existe}\ (u, v) \in E\}$$

Ele é chamado de *lista de sucessores* ou *lista de adjacências* de u.

A *representação gráfica* de um grafo orientado G é uma representação de G no plano. Isto é, cada vértice u de G é representado por um ponto (ou um pequeno círculo), e cada aresta (orientada) $e = (u, v)$ é representada por uma seta ou curva orientada do ponto inicial u de e para o ponto terminal v. Em geral, um dígrafo G é mais comumente representado por sua representação do que pela listagem explícita de seus vértices e arestas.

Se as arestas e/ou vértices de um grafo orientado G são rotuladas com algum tipo de dado, então G é dito um *grafo orientado rotulado*.

Um grafo orientado $G(V, E)$ é dito *finito* se o seu conjunto de vértices V e o seu conjunto de arestas E são finitos.

Exemplo 9.1

(*a*) Considere o grafo orientado G desenhado na Figura 9-1. Ele consiste em quatro vértices e sete arestas como a seguir:

$$V(G) = \{A, B, C, D\}$$
$$E(G) = \{e_1, \ldots, e_7\} = \{(A, D), (B, A), (B, A), (D, B), (B, C), (D, C), (B, B)\}$$

As arestas e_2 e e_3 são ditas paralelas, já que ambas começam em B e terminam em A. A aresta e_7 é um laço, já que começa e termina em B.

(*b*) Suponha que três garotos, A, B e C, estejam jogando bola um para o outro de tal modo que A sempre joga a bola para B, mas B e C jogam a bola para A com a mesma probabilidade que o fazem um para o outro. A Figura 9-2 ilustra esse sistema dinâmico em que as arestas estão rotuladas com as respectivas probabilidades, i.e., A joga a bola para B com probabilidade 1, B joga a bola para A e C com probabilidade $\frac{1}{2}$, e C joga a bola para A e B com probabilidade $\frac{1}{2}$.

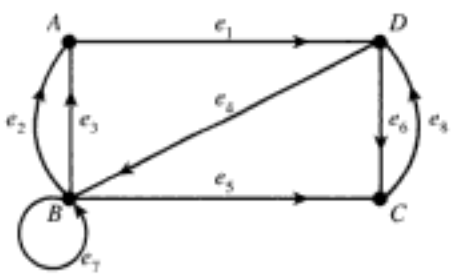


Fig. 9-1

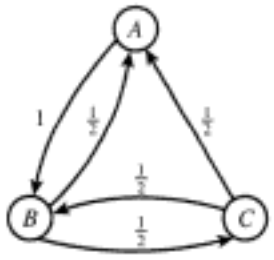


Fig. 9-2

Subgrafos

Seja $G = G(V, E)$ um grafo orientado, e seja V' um subconjunto de V de vértices de G. Suponha que E' é um subconjunto de E tal que os pontos finais das arestas em E' pertencem a V'. Então, $H(V', E')$ é um grafo orientado e é dito um *subgrafo* de G. Em particular, se E' contém todas as arestas em E cujos pontos finais pertencem a V', então $H(V', E')$ é dito o subgrafo de G *gerado* ou *determinado* por V'. Por exemplo, considere o grafo $G = G(V, E)$ da Figura 9-1. Seja

$$V' = \{B, C, D\} \qquad \text{e} \qquad E' = \{e_4, e_5, e_6, e_7\} = \{(D, B), (B, C), (D, C), (B, B)\}$$

Então, $H(V', E')$ é o subgrafo de G determinado pelo conjunto de vértices E'.

9.3 DEFINIÇÕES BÁSICAS

Esta seção discute as questões relativas a grau de vértices, caminhos e conectividade em grafos orientados.

Graus

Suponha que G é um grafo orientado. O grau de saída de um vértice v de G (escreve-se $d^+(v)$[†]) é o número de arestas começando em v, e o grau de entrada (escreve-se $d^-(v)$[††]) é o número de arestas terminando em v. Como cada aresta começa e termina em um vértice, obtemos imediatamente o teorema seguinte.

Teorema 9-1: a soma dos graus de saída dos vértices de um grafo orientado G é igual à soma dos graus de entrada dos vértices, que é igual ao número de arestas em G.

Um vértice v com grau de entrada zero é dito uma *fonte*, e um vértice v com grau de saída zero é dito um *sumidouro*.

Exemplo 9.2 Considere o grafo G da Figura 9-1. Temos

$$d^+(v)\ (A) = 1, \quad d^+(v)\ (B) = 4, \quad d^+(v)\ (C) = 0, \quad d^+(v)\ (D) = 2$$
$$d^-(v)\ (A) = 2, \quad d^-(v)\ (B) = 2, \quad d^-(v)\ (C) = 2, \quad d^-(v)\ (D) = 1$$

Como era de se esperar, a soma dos graus de saída é igual à soma dos graus de entrada, que é igual ao número de arestas, sete. O vértice C é um sumidouro, uma vez que nenhuma aresta começa em C. O grafo não tem fontes.

Caminhos

Seja G um grafo orientado. Os conceitos de caminho, caminho simples, trilha e ciclo são os mesmos dos grafos não orientados, exceto pelo fato de que a direção da aresta deve coincidir com a direção do caminho. Especificamente,

(i) Um *caminho* (*orientado*) P em G é uma seqüência alternada de vértices e arestas orientadas, por exemplo,

$$P = (v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n)$$

tal que cada aresta e_i começa em v_{i-1} e termina em v_i. Quando não existem ambigüidades, denotamos P por sua seqüência de vértices ou por sua seqüência de arestas.

(ii) O *comprimento* do caminho P é n, seu número de arestas.

(iii) Um *caminho simples* é um caminho com vértices distintos. Uma *trilha* é um caminho com arestas distintas.

(iv) Um *caminho fechado* tem os vértices primeiro e último iguais.

(v) Um *caminho gerador* contém todos os vértices de G.

(vi) Um *ciclo* (ou *circuito*) é um caminho fechado com vértices distintos (exceto o primeiro e o último).

(vii) Um *semicaminho* é o mesmo que um caminho, a não ser pelo fato de que a aresta e_i pode iniciar em v_{i-1} ou v_i e terminar no outro vértice. *Semitrilhas* e caminhos *semi-simples* são definidos de maneira análoga.

Um vértice v é *alcançável* a partir de um vértice u se existir um caminho de u para v. Se v é alcançável a partir de u, então (eliminando as arestas redundantes) existe um caminho simples de u para v.

Exemplo 9.3 Considere o grafo G da Figura 9-1.

(*a*) A seqüência $P_1 = (D, C, B, A)$ é um semicaminho, mas não é um caminho, pois (C, B) não é uma aresta; isto é, a direção de $e_5 = (C, B)$ não concorda com a direção de P_1.

(*b*) A seqüência $P_2 = (D, B, A)$ é um caminho de D para A, uma vez que (D, B) e (B, A) são arestas. Portanto, A é alcançável a partir de D.

Conectividade

Existem três tipos de conectividade em um grafo orientado G:

(i) G é *fortemente conexo* ou *forte* se, para qualquer par de vértices u e v em G, existe um caminho de u para v e um caminho de v para u, isto é, se cada um deles é alcançável a partir do outro.

(ii) G é *unilateralmente conexo* ou *unilateral*, se para qualquer par de vértices u e v em G, existe um caminho de u para v ou um caminho de v para u, isto é, se algum deles é alcançável a partir do outro.

(iii) G é *fracamente conexo* ou *fraco* se existe um semicaminho entre quaisquer dois vértices u e v em G.

[†] N. de T. No original, *outdeg*(v).

[††] N. de T. No original, *indeg*(v).

Seja G' um grafo (não orientado), obtido do grafo orientado G considerando todas as arestas de G como não orientadas. Claramente, G é fracamente conexo se e somente se o grafo G' é conexo.

Observe que conectividade forte implica conectividade unilateral, e que conectividade unilateral implica conectividade fraca. Dizemos que G é *estritamente unilateral* se é unilateral mas não forte, e é *estritamente fraco* se é fraco mas não unilateral.

Conectividade pode ser caracterizada em termos de caminhos geradores, como a seguir.

Teorema 9-2: seja G um grafo orientado finito. Então,

(i) G é fortemente conexo se e somente se tem um caminho gerador fechado.
(ii) G é unilateralmente conexo se e somente se tem um caminho gerador.
(iii) G é fracamente conexo se e somente se tem um semicaminho gerador.

Exemplo 9.4 Considere o grafo G da Figura 9-1. Ele é fracamente conexo, uma vez que o grafo não orientado subjacente é conexo. Não existe caminho de C para nenhum outro vértice (i.e., C é um sumidouro), logo, G não é fortemente conexo. Entretanto, $P = (B, A, D, C)$ é um caminho gerador e, logo, G é unilateralmente conexo.

Grafos com fontes e sumidouros aparecem em muitas aplicações (por exemplo, diagramas de fluxos e redes). A condição seguinte é suficiente para a existência de tais vértices.

Teorema 9-3: suponha que um grafo orientado finito G é acíclico, isto é, não contém nenhum ciclo (orientado). Então, G contém uma fonte ou um sumidouro.

Prova: Seja $P = (v_0, v_1, \ldots, v_n)$ um caminho simples de comprimento máximo, que existe por G ser finito. Então, o último vértice v_n é um sumidouro; por outro lado, uma aresta (v_n, u) irá estender P ou formar um ciclo se $u = v_i$ para algum i. De modo semelhante, o primeiro vértice v_0 é uma fonte.

9.4 ÁRVORES COM RAÍZES

Lembre que uma árvore é um grafo conexo acíclico, isto é, um grafo conexo sem ciclos. Uma *árvore com raiz* (ou *enraizada*) T é uma árvore que contém um vértice designado r, chamado de *raiz* da árvore. Como existe um único caminho simples da raiz r para qualquer outro vértice v em T, isso determina a direção das arestas de T. Portanto, T pode ser visto como um grafo orientado. Notamos que qualquer árvore pode ser transformada em uma árvore com raiz pela simples seleção de um dos vértices como a raiz.

Considere uma árvore T com raiz r. O comprimento do caminho da raiz r para qualquer vértice v é dito o *nível* (ou *profundidade*) de v, e o maior nível de vértice é dito a *profundidade* da árvore. Os vértices com grau 1, diferentes da raiz r, são ditos as *folhas* de T, e o caminho orientado de um vértice até uma folha é dito um *ramo*.

Normalmente desenha-se a figura de uma árvore com raiz T com a raiz no topo da árvore. A Figura 9-3 mostra uma árvore T com raiz r e 10 outros vértices. A árvore tem cinco folhas, d, f, h, i e j. Observe que:

$$\text{nível } (a) = 1, \qquad \text{nível } (f) = 2, \qquad \text{nível } (j) = 3$$

Além disso, a profundidade da árvore é 3.

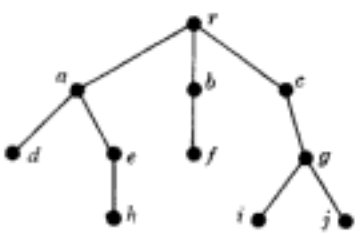


Fig. 9-3

O fato de uma árvore com raiz T indicar a direção das arestas significa que podemos definir uma relação de precedência entre os vértices. Especificamente, diremos que um vértice u *precede* um vértice v ou que v *segue* u se existe um caminho (orientado) de u para v. Em particular, dizemos que v *segue imediatamente* u se (u, v) é uma aresta, isto é, se v segue u e é adjacente a u.

Notamos que todo vértice v, a menos da raiz, segue imediatamente um único vértice, mas que v pode ser seguido imediatamente por mais de um vértice. Por exemplo, na Figura 9-3, o vértice j segue c, mas segue imediatamente g. Além disso, i e j seguem imediatamente g.

Uma árvore com raiz T também é um dispositivo útil para enumerar todas as possibilidades lógicas de uma seqüência de eventos em que cada evento pode ocorrer de um número finito de maneiras. Isso está ilustrado no exemplo seguinte.

Exemplo 9.5 Suponha que Marcos e Érico estão disputando um torneio de tênis tal que a primeira pessoa que ganhar dois jogos seguidos ou um total de três jogos, ganha o torneio. Ache o número de maneiras pelas quais o torneio pode acontecer.

A árvore enraizada na Figura 9-4 (cuja raiz está à esquerda) mostra as várias possibilidades. Existem 10 folhas que correspondem às 10 maneiras pelas quais o torneio pode ocorrer:

MM, MEMM, MEMEM, MEMEE, MEE, EMM, EMEMM, EMEME, EMEE, EE

Especificamente, o caminho da raiz para folha descreve quem ganha qual jogo no torneio.

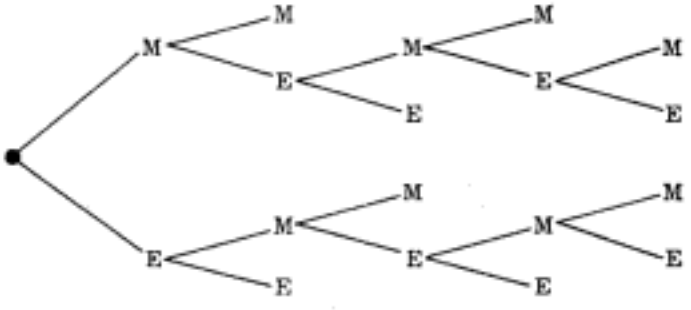


Fig. 9-4

Árvores Enraizadas Ordenadas

Considere uma árvore enraizada T na qual as arestas que deixam cada vértice são ordenadas. Temos então o conceito de *árvore enraizada* (ou *com raiz*) *ordenada*. É possível rotular (ou *atribuir endereços*) de forma sistemática aos vértices de uma tal árvore como a seguir: primeiramente atribuímos 0 à raiz r. Depois, atribuímos 1, 2, 3,... aos vértices que imediatamente seguem r de acordo com a ordenação das arestas. Então, rotulamos os vértices remanescentes da maneira descrita a seguir. Se a é o rótulo de um vértice v, então $a.1$, $a.2$,... são atribuídos aos vértices que seguem v imediatamente, de acordo com a ordenação das arestas. Ilustramos este sistema de endereçamento na Figura 9-5, onde as arestas estão representadas da esquerda para a direita de acordo com sua ordem. Observe que o número de pontos em qualquer rótulo é um a menos que o nível do vértice. Vamos nos referenciar a este sistema de rotulação como *sistema de endereçamento universal* para uma árvore enraizada ordenada.

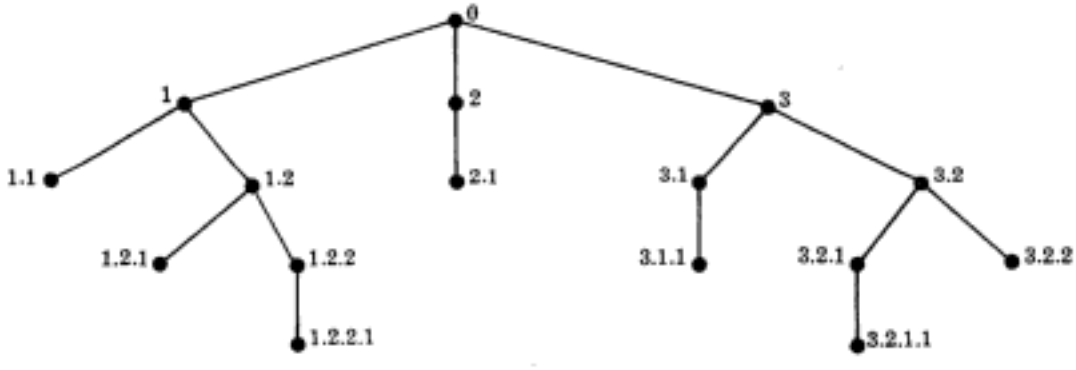
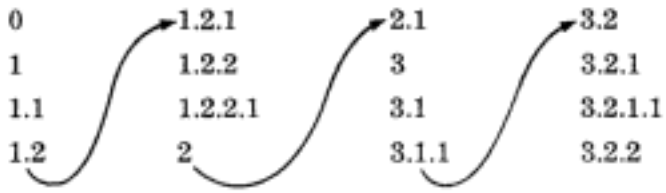


Fig. 9-5

O sistema de endereçamento universal nos fornece uma maneira importante de descrever linearmente (ou armazenar) uma árvore rotulada ordenada. Especificamente, dados os endereços a e b, fazemos $a < b$ se a é um *segmento inicial* de b, i.e., se $b = a.c$, ou se existem inteiros positivos m e n com $m < n$ tais que

$$a = r.m.s \quad \text{e} \quad b = r.n.t$$

Essa ordem é chamada *ordem lexicográfica*, já que é semelhante à maneira pela qual palavras são ordenadas em um dicionário. Por exemplo, os endereços na Figura 9-5 estão ordenados linearmente como a seguir:



A ordem lexicográfica é idêntica à ordem obtida movendo para baixo o ramo mais à esquerda da árvore, depois o primeiro ramo à direita, depois o segundo ramo à direita, e assim por diante.

Expressões Algébricas e Notação Polonesa

Toda expressão algébrica envolvendo operações binárias, por exemplo, adição, subtração, multiplicação e divisão, pode ser representada por uma árvore ordenada enraizada. Por exemplo, a Figura 9-6(a) representa a expressão aritmética

$$(a - b)/((c \times d) + e) \tag{9.1}$$

Observe que as variáveis na expressão a, b, c, d e e aparecem como folhas, e as operações aparecem como os outros vértices. A árvore precisa ser ordenada, já que $a - b$ e $b - a$ geram a mesma árvore mas não a mesma árvore ordenada.

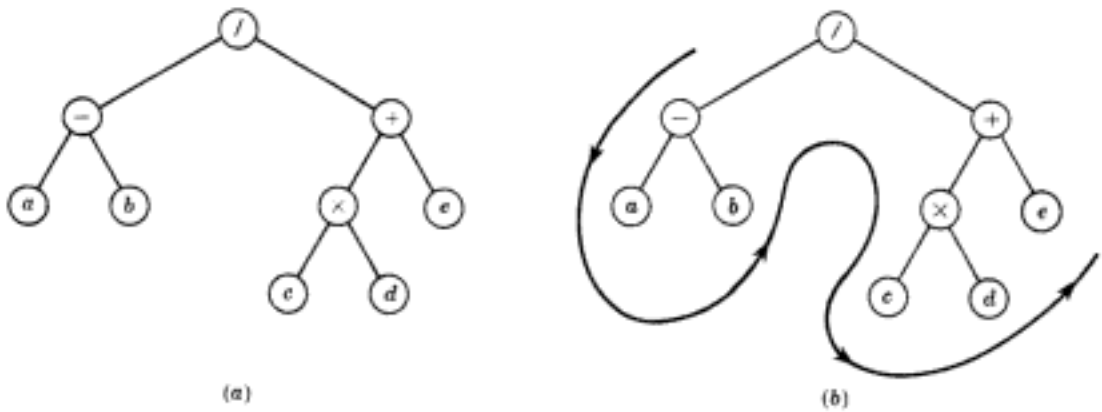


Fig. 9-6

O matemático polonês Lukasiewicz observou que colocando o símbolo de operação binária antes dos argumentos, por exemplo,

$$+ab \text{ em vez de } a + b \qquad \text{e} \qquad /cd \text{ em vez de } c/d$$

não é necessário usar parênteses. Essa notação é chamada *notação polonesa na forma prefixa* (analogamente pode-se colocar o símbolo depois dos argumentos, e teremos a notação conhecida como notação polonesa na forma posfixa). Rescrevendo (9.1) na forma prefixa, obtemos

$$/ - ab + \times cde$$

Observe que esta é precisamente a ordem lexicográfica dos vértices, que pode ser obtida representando a árvore como na Figura 9-6(b).

9.5 REPRESENTAÇÃO SEQÜENCIAL DE GRAFOS ORIENTADOS

Existem duas maneiras de manter um grafo orientado na memória de um computador. Uma maneira, chamada *representação seqüencial* de G, é por meio da matriz de adjacências A. A outra maneira, dita a *representação ligada* de G, é por listas ligadas de vizinhanças. Esta seção cobre a primeira representação e mostra como a matriz de adjacências A de G pode ser usada para responder facilmente a certas questões de conectividade em G. A representação ligada será tratada na Seção 9-7.

Suponha que um grafo G tem m vértices (nós) e n arestas. Dizemos que G é *denso* se $m = O(n^2)$, e *esparso* se $m = O(n)$ ou ainda se $m = O(n \log n)$. A representação matricial de G é normalmente usada se G é denso, e listas ligadas são mais comuns se G é esparso. Independentemente da forma como um grafo G é mantido na memória do computador, sua entrada se dá pela sua definição formal, isto é, como uma coleção de vértices e uma coleção de arestas (pares ordenados de vértices).

Observação: A fim de evitar casos particulares de nossos resultados, sempre vamos assumir, a menos que haja observação em contrário, que $m > 1$, onde m é o número de vértices do nosso grafo G. Portanto, G não pode ser conexo se não tiver arestas.

Dígrafos e Relações, Matrizes de Adjacências

Seja $G(V, E)$ um grafo orientado *simples*, isto é, um grafo sem arestas paralelas. Então, E é simplesmente um subconjunto de $V \times V$, e, portanto, E é uma relação em V. Conversamente, se R é uma relação em um conjunto V, então $G(V, R)$ é um grafo orientado simples. Logo, os conceitos de relações em um conjunto e de grafos orientados simples são um só. De fato, no Capítulo 2, já apresentamos o grafo orientado correspondente à uma relação em um conjunto.

Suponha que G é um grafo orientado simples com m vértices, e suponha que os vértices de G tenham sido ordenados e são denominados como $v_1, v_2, \ldots, v_m$. Então, a *matriz de adjacências* $A = [a_{ij}]$ de G é a matriz $m \times m$ definida como a seguir:

$$a_{ij} = \begin{cases} 1 & \text{se existe uma aresta } (v_i, v_j) \\ 0 & \text{caso contrário} \end{cases}$$

Uma tal matriz A, cujos únicos elementos são 0 e 1, é chamada *matriz bit* ou *matriz booleana*.

A matriz de adjacências A do grafo G depende da ordem dos vértices de G, isto é, uma ordenação diferente dos vértices pode resultar em uma matriz de adjacências diferente. Entretanto, as matrizes de adjacências resultantes de diferentes ordenações de vértices estão relacionadas intimamente, e uma pode ser obtida a partir da outra pela troca de linhas ou colunas. A menos que haja observação em contrário, vamos assumir que os vértices da matriz tenham uma ordem fixa.

Observação 1: A matriz de adjacências $A = [a_{ij}]$ pode ser estendida para grafos orientados com arestas paralelas fazendo

$$a_{ij} = \text{número de arestas começando em } v_i \text{ e terminando em } v_j$$

Neste caso, os elementos de A serão inteiros não negativos. Conversamente, toda matriz A $m \times m$ define de maneira única um grafo orientado com m vértices.

Observação 2: Se G é um grafo não orientado, então a matriz de adjacências A de G é uma matriz simétrica, i. e., $a_{ij} = a_{ji}$ para todo i e j. Isto decorre do fato de que cada aresta não orientada $\{u, v\}$ corresponde a duas arestas orientadas: (u, v) e (v, u).

Exemplo 9.6 Considere o grafo orientado G da Figura 9-7 com vértices X, Y, Z e W. Suponha que os vértices são ordenados como a seguir:

$$v_1 = X, \qquad v_2 = Y, \qquad v_3 = Z, \qquad v_4 = W$$

Então, a matriz de adjacências A de G é:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Note que a quantidade de números 1 em A é igual ao número (oito) de arestas.

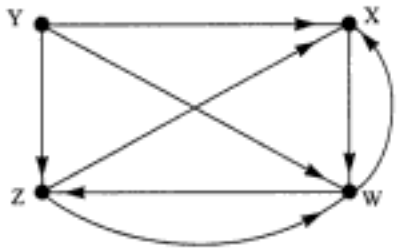


Fig. 9-7

Considere as potências A, A^2, A^3, ... da matriz de adjacências $A = [a_{ij}]$ do grafo G. Usaremos a notação

$$a_K(i,j) = \text{elemento } ij \text{ da matriz } A^K$$

Note que $a_1(i,j) = a_{ij}$ dá o número de caminhos de comprimento 1 do vértice v_i para o vértice v_j. Pode-se mostrar que $a_2(i,j)$ dá o número de caminhos de comprimento 2 de v_i para v_j. De fato, provamos no Problema 9.14 que vale o resultado geral enunciado a seguir.

Proposição 9-4: Seja A a matriz de adjacências de um grafo G. Então, $a_K(i,j)$, o elemento ij da matriz A^K, dá o número de caminhos de comprimento K de v_i para v_j.

Exemplo 9.7 Considere novamente o grafo G da Figura 9-7, cuja matriz de adjacências A é dada no Exemplo 9.6. As potências A^2, A^3 e A^4 de A são:

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 2 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 1 & 0 & 0 & 2 \\ 3 & 0 & 2 & 3 \\ 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 2 & 0 & 2 & 1 \\ 5 & 0 & 3 & 5 \\ 3 & 0 & 2 & 3 \\ 3 & 0 & 1 & 4 \end{bmatrix}$$

Observe que $a_2(4,1) = 1$, pois existe um caminho de comprimento 2 de v_4 para v_1. Também, $a_3(2,3) = 2$, pois existe um caminho de comprimento 3 de v_2 para v_3; e $a_4(2,4) = 5$, pois existe um caminho de comprimento 4 de v_2 para v_4. (Aqui, $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$.)

Observação: Suponha que A é a matriz de adjacências de um grafo G, e suponha que agora definimos a matriz B como

$$B_r = A + A^2 + A^3 + \cdots + A^r$$

Então, o elemento ij da matriz B_r dá o número de caminhos, de comprimento r ou menor, do vértice v_i para o vértice v_j.

Matriz de Caminhos

Seja $G = G(V, E)$ um grafo orientado simples com m vértices $v_1, v_2, \ldots, v_m$. A *matriz de caminhos* ou *matriz de acessibilidade* de G é a matriz quadrada $m \times m$ $P = (p_{ij})$ definida como:

$$p_{ij} = \begin{cases} 1 & \text{se existe um caminho de } v_i \text{ para } v_j \\ 0 & \text{caso contrário} \end{cases}$$

(A próxima subseção mostra que a matriz de caminhos P pode ser considerada como o fecho transitivo da relação E em V).

Suponha agora que existe um caminho de um vértice v_i para um vértice v_j em um grafo G com m vértices. Então, deve existir um caminho simples de v_i para v_j quando $v_i \neq v_j$, ou deve haver um ciclo de v_i para v_j se $v_i = v_j$. Como G tem m vértices, este caminho simples deve ter comprimento menor ou igual a $m - 1$, ou o ciclo deve ter comprimento m ou menor. Isto quer dizer que existe um elemento ij não-nulo na matriz

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

onde A é a matriz de adjacências de G. Conseqüentemente, a matriz de caminhos P e B_m têm elementos não-nulos nas mesmas posições ij. Declaramos formalmente esse resultado.

Proposição 9-5: Seja A a matriz de adjacências de um grafo G com m vértices, e seja

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Então, a matriz de caminhos P e B_m tem elementos não nulos nas mesmas posições.

Lembre que um grafo orientado G é dito *fortemente conexo* se, para qualquer par de vértices u e v em G, existe um caminho de u para v e um caminho de v para u. Conseqüentemente, G é fortemente conexo se e somente se a matriz de caminhos P de G não tem elementos nulos. Esse fato, juntamente com a Proposição 9.5, permite concluir o resultado seguinte.

Proposição 9-6: Seja A a matriz de adjacências de um grafo G com m vértices, e seja

$$B_m = A + A^2 + A^3 + \cdots + A^m$$

Então, G é fortemente conexo se e somente se B_m não tem elementos nulos.

Exemplo 9.8 Considere o grafo G com $m = 4$ vértices da Figura 9-7, e sejam $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. Adicionando as matrizes A, A^2, A^3, A^4 nos Exemplos 9.6 e 9.7, obtemos a seguinte matriz B_4, e, substituindo os elementos não-nulos em B_4 por 1, obtemos a matriz de caminhos (acessibilidade) P do grafo G:

$$B_4 = \begin{bmatrix} 4 & 0 & 3 & 4 \\ 11 & 0 & 7 & 11 \\ 7 & 0 & 4 & 7 \\ 7 & 0 & 4 & 7 \end{bmatrix} \quad \text{e} \quad P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Examinando a matriz B_4 ou P, observamos elementos nulos; portanto, G não é fortemente conexo. Em particular, vemos que o vértice $v_2 = Y$ não é alcançável a partir de nenhum dos outros vértices.

Observação: A matriz de adjacências A e a matriz de caminhos P de um grafo G podem ser encaradas como matrizes lógicas (booleanas) onde 0 representa "Falso" e 1 representa "Verdadeiro". Portanto, as operações lógicas $\wedge$ (E) e $\vee$ (OU), cujos valores aparecem na Figura 9-8, podem ser aplicadas aos elementos de A e P. Essas operações serão usadas na próxima seção.

$\wedge$	0	1
0	0	0
1	0	1

(*a*) E

$\vee$	0	1
0	0	1
1	1	1

(*b*) OU

Fig. 9-8

Fecho Transitivo e Matriz de Caminhos

Seja R uma relação em um conjunto finito V com m elementos. Como observado acima, a relação R pode ser identificada com o grafo simples orientado $G = G(V, R)$. Lembre (Seção 2.5) que a composição de relações $R^2 = R \circ R$ é definida por

$$R^2 = \{(u, v): \exists\ w \in V \text{ tal que } (u, w) \in R \text{ e } (w, v) \in R\}$$

Em outras palavras, R^2 consiste em todos os pares (u, v) tais que existe um caminho de comprimento 2 de u para v. v. Analogamente,

$$R^K = \{(u, v): \text{existe um caminho de comprimento } K \text{ de } u \text{ para } v\}.$$

O fecho transitivo R^* da relação R em V pode agora ser encarado como o conjunto de pares ordenados (u, v), tais que existe um caminho de u para v no grafo G. Conseqüentemente, a matriz de caminhos P de $G = G(V, R)$ é precisamente a matriz de adjacências do grafo $G' = G'(V, R^*)$ que corresponde ao fecho transitivo R^*. Além disto, pela discussão acima, precisamos olhar apenas para os caminhos simples de comprimento menor ou igual a $m - 1$ e ciclos de comprimento m ou menor. Conseqüentemente, temos o resultado seguinte, que caracteriza o fecho transitivo R^* de R.

Teorema 9-7: Seja R uma relação em um conjunto V com m elementos. Então:

(i) $R^* = R \cup R^2 \cup \cdots \cup R^m$ é o fecho transitivo de R.

(ii) A matriz de caminhos P de $G(V, R)$ é a matriz de adjacências de $G'(V, R^*)$.

9.6 ALGORITMO DE WARSHALL; CAMINHO MÍNIMO

Seja G um grafo orientado com m vértices $v_1, v_2, \ldots, v_m$. Suponha que queiramos achar a matriz de caminhos P do grafo G. Warshall propôs um algoritmo que é muito mais eficiente do que calcular as potências da matriz de adjacências A. Esse algoritmo está definido nesta seção, e um algoritmo similar é usado para determinar os caminhos mínimos em G quando G é ponderado.

Algoritmo de Warshall

Primeiro definimos as matrizes booleanas quadradas $m \times m$ $P_0, P_1, \ldots, P_m$ como a seguir. Seja $P_k[i, j]$ o elemento ij da matriz P_k. Então definimos:

$$P_k[i, j] = \begin{cases} 1 & \text{se existe um caminho simples de } v_i \text{ para } v_j \text{ que não usa nenhum outro vértice exceto} \\ & \text{possivelmente } v_1, v_2, \ldots, v_k \\ 0 & \text{caso contrário} \end{cases}$$

Isto é,

$P_0[i, j] = 1$ se existe uma aresta de v_i para v_j

$P_1[i, j] = 1$ se existe um caminho simples de v_i para v_j que não usa nenhum outro vértice exceto possivelmente v_1

$P_2[i, j] = 1$ se existe um caminho simples de v_i para v_j que não usa nenhum outro vértice exceto possivelmente v_1 e v_2

E assim sucessivamente.

Observe que a primeira matriz $P_0 = A$, a matriz de adjacências de G. Além disso, como G tem apenas m vértices, a última matriz $P_m = P$, a matriz de caminhos de G.

Warshall observou que $P_k[i, j] = 1$ pode ocorrer apenas se um dos seguintes dois casos ocorrer:

(1) Existe um caminho simples de v_i para v_j que não usa nenhum outro vértice exceto possivelmente $v_1, v_2, \ldots, v_{k-1}$; logo,

$$P_{k-1}[i, j] = 1$$

(2) Existe um caminho simples de v_i para v_k e um caminho simples de v_k para v_j onde cada caminho simples não usa nenhum outro vértice exceto possivelmente $v_1, v_2, \ldots, v_{k-1}$; logo,

$$P_{k-1}[i,k] = 1 \qquad \text{e} \qquad P_{k-1}[k,j] = 1$$

Esses dois casos estão representados por:

$$(1) \quad v_i \to \cdots \to v_j; \qquad (2) \quad v_i \to \cdots \to v_k \to \cdots \to v_j$$

Aqui,

$$\to \cdots \to$$

denota a parte de um caminho simples que não usa nenhum outro vértice exceto possivelmente $v_1, v_2, \ldots, v_{k-1}$. Conseqüentemente, os elementos de P_k podem ser obtidos por

$$P_k[i,j] \;=\; P_{k-1}[i,j] \;\vee\; (P_{k-1}[i,k] \wedge P_{k-1}[k,j])$$

onde usamos as operações lógicas $\wedge$ (E) e $\vee$ (OU). Em outras palavras, podemos obter cada elemento da matriz P_k considerando apenas três elementos da matriz P_{k-1}. O algoritmo de Warshall vem a seguir.

Algoritmo 9.6: (**Algoritmo de Warshal**) Um grafo orientado G com M vértices é representado na memória pela sua matriz de adjacências A. O algoritmo determina a matriz (booleana) de caminhos P do grafo G.

Passo 1 Repita para $I, J = 1, 2, \ldots, M$: [Inicializa P.]
Se $A[I, J] = 0$, então: faça $P[I, J]$: $= 0$;
Senão: faça $P[I, J]$: $= 1$.
[Fim do *loop*.]

Passo 2 Repita os Passos 3 e 4 para $K = 1, 2, \ldots, M$: [Atualiza P.]

Passo 3 Repita o Passo 4 para $I = 1, 2, \ldots, M$:

Passo 4 Repita para $J = 1, 2, \ldots, M$
Faça $P[I, J]$: $= P[I, J] \vee (P[I, K] \wedge P[K, J])$.
[Fim o *loop*.]
[Fim do *loop* do Passo 3.]
[Fim do *loop* do Passo 2.]

Passo 5 Saia.

Algoritmos para Caminho Mínimo

Seja G um grafo orientado simples com m vértices, $v_1, v_2, \ldots, v_m$. Suponha que G é ponderado; isto é, suponha que se atribui a cada aresta e de G um número não negativo $w(e)$, denominado o *peso* ou *comprimento* de e. Então, G pode ser mantido na memória pela sua *matriz de pesos* $W = (w_{ij})$ definida por

$$w_{ij} = \begin{cases} w(e) & \text{se existe uma aresta } e \text{ de } v_i \text{ para } v_j \\ 0 & \text{se não existe uma aresta de } v_i \text{ para } v_j \end{cases}$$

A matriz de caminhos P nos diz se existem ou não caminhos entre os vértices. Agora, queremos determinar a matriz Q, que nos diz os comprimentos dos caminhos mínimos entre os vértices ou, mais precisamente, a matriz $Q = (q_{ij})$ onde

$$q_{ij} = \text{comprimento do menor caminho de } v_i \text{ para } v_j$$

Descrevemos a seguir uma modificação do algoritmo de Warshall para determinar a matriz Q de maneira eficiente.

Definimos uma seqüência de matrizes $Q_0, Q_1, \ldots, Q_m$ (análogas às matrizes anteriormente definidas $P_0, P_1, \ldots, P_m$) onde $Q_k[i,j]$, o elemento ij de Q_k, é definido como a seguir.

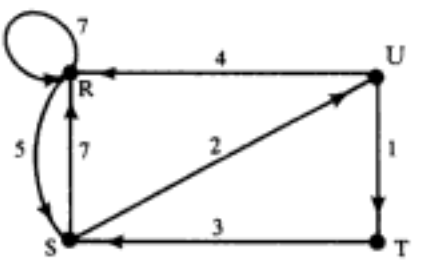
$Q_k[i,j]$ = menor valor entre comprimento do caminho precedente de v_i para v_j ou a soma dos comprimentos dos caminhos precedentes de v_i para v_k e de v_k para v_j.

Mais exatamente,

$$Q_k[i,j] = \text{MIN}\,(Q_{k-1}[i,j],\ Q_{k-1}[i,k] + Q_{k-1}[k,j])$$

A matriz inicial Q_0 é a mesma que a matriz de pesos W, exceto pelo fato de que cada 0 em W é substituído por ∞ (ou um número muitíssimo grande). A matriz final Q_m será a matriz procurada Q.

Exemplo 9.9 A Figura 9-9 mostra um grafo ponderado G e sua matriz de pesos W, onde assumimos $v_1 = R,\ v_2 = S,\ v_3 = T,\ v_4 = U$.



$$W = \begin{bmatrix} 7 & 5 & 0 & 0 \\ 7 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{bmatrix}$$

Fig. 9-9

Suponha que apliquemos o algoritmo de Warshall modificado ao nosso grafo ponderado G. Obteremos as matrizes Q_0, Q_1, Q_2, Q_3 e Q_4 na Figura 9-10. (À direita de cada matriz Q_k, na Figura 9-10, mostramos a matriz dos caminhos que correspondem aos comprimentos na matriz Q_k.) Os elementos na matriz Q_0 são os mesmos que na matriz W, exceto pelo fato de que cada 0 em W é substituído por ∞ (um número muito grande). Indicamos como os elementos circundados são obtidos:

$$Q_1[4,2] = \text{MIN}\,(Q_0[4,2], Q_0[4,1] + Q_0[1,2]) = \text{MIN}\,(\infty, 4+5) = 9$$
$$Q_2[1,3] = \text{MIN}\,(Q_1[1,3], Q_1[1,2] + Q_1[2,3]) = \text{MIN}\,(\infty, 5+\infty) = \infty$$
$$Q_3[4,2] = \text{MIN}\,(Q_2[4,2], Q_2[4,3] + Q_2[3,2]) = \text{MIN}\,(9, 3+1) = 4$$
$$Q_4[3,1] = \text{MIN}\,(Q_3[3,1], Q_3[3,4] + Q_3[4,1]) = \text{MIN}\,(10, 5+4) = 9$$

A última matriz $Q_4 = Q$ é a matriz procurada do caminho mínimo.

$$Q_0 = \begin{pmatrix} 7 & 5 & \infty & \infty \\ 7 & \infty & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \infty & 1 & \infty \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & — \\ \text{SR} & — & — & \text{SU} \\ — & \text{TS} & — & — \\ \text{UR} & — & \text{UT} & — \end{pmatrix}$$

$$Q_1 = \begin{pmatrix} 7 & 5 & \infty & \infty \\ 7 & 12 & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \textcircled{9} & 1 & \infty \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & — \\ \text{SR} & \text{SRS} & — & \text{SU} \\ — & \text{TS} & — & — \\ \text{UR} & \text{URS} & \text{UT} & — \end{pmatrix}$$

$$Q_2 = \begin{pmatrix} 7 & 5 & \textcircled{\infty} & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & 9 & 1 & 11 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & \text{RSU} \\ \text{SR} & \text{SRS} & — & \text{SU} \\ \text{TSR} & \text{TS} & — & \text{TSU} \\ \text{UR} & \text{URS} & \text{UT} & \text{URS} \end{pmatrix}$$

Fig. 9-10 (1 de 2)

$$Q_3 = \begin{pmatrix} 7 & 5 & \infty & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & \textcircled{4} & 1 & 6 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & — & \text{RSU} \\ \text{SR} & \text{SRS} & — & \text{SU} \\ \text{TSR} & \text{TS} & — & \text{TSU} \\ \text{UR} & \text{UTS} & \text{UT} & \text{UTSU} \end{pmatrix}$$

$$Q_4 = \begin{pmatrix} 7 & 5 & 8 & 7 \\ 7 & 11 & 3 & 2 \\ \textcircled{9} & 3 & 6 & 5 \\ 4 & 4 & 1 & 6 \end{pmatrix} \qquad \begin{pmatrix} \text{RR} & \text{RS} & \text{RSUT} & \text{RSU} \\ \text{SR} & \text{SURS} & \text{SUT} & \text{SU} \\ \text{TSUR} & \text{TS} & \text{TSUT} & \text{TSU} \\ \text{UR} & \text{UTS} & \text{UT} & \text{UTSU} \end{pmatrix}$$

Fig. 9-10 (2 de 2)

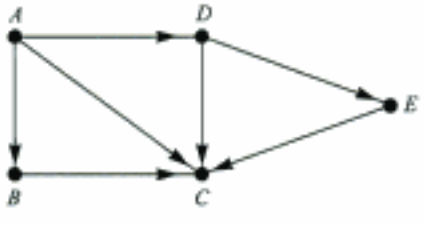
9.7 REPRESENTAÇÃO LIGADA DE GRAFOS ORIENTADOS

Seja G um grafo com m vértices. Suponha que o número de arestas de G é $O(m)$ ou mesmo $O(m \log m)$, isto é, suponha que G é esparso. Então, a matriz de adjacências A de G conterá muitos zeros; logo, uma grande quantidade de espaço de memória será desperdiçada. Conseqüentemente, quando G é esparso, normalmente é representado na memória por algum tipo de *representação ligada*, também chamada *estrutura de adjacências*, que está descrita abaixo por meio de um exemplo.

Considere o grafo orientado G na Figura 9-11(a). Observe que G pode ser definido de modo equivalente pela tabela na Figura 9-11(b), que mostra cada vértice em G seguido por sua *lista de adjacências*, também chamadas de *sucessores* ou *vizinhos*. Aqui, o símbolo ∅ denota uma lista vazia. Observe que cada aresta de G corresponde a um único vértice na lista de adjacências e vice-versa. Aqui, G tem sete arestas, e existem sete vértices nas listas de adjacências. Essa tabela também pode ser apresentada na forma compacta

$$G = [A{:}B, C, D;\quad B{:}C;\quad C{:}\varnothing;\quad D{:}C, E;\quad E{:}C]$$

onde o símbolo dois-pontos ":" separa um vértice da sua lista de vizinhos, e ponto-e-vírgula, ";", separa listas distintas.



(a) Grafo G

Vértice	Lista de adjacências
A	B, C, D
B	C
C	∅
D	C, E
E	C

(b) Lista de adjacências de G

Fig. 9-11

A *representação ligada* de um grafo orientado G mantém G na memória usando listas ligadas para suas listas de adjacências. Especificamente, a representação ligada conterá normalmente dois arquivos (conjuntos de registros), um chamado arquivo de vértices e outro chamado arquivo de arestas, como indicado a seguir.

(a) ***Arquivo de vértices***: o arquivo de vértices conterá a lista de vértices do grafo G normalmente armazenada em um *array* ou em uma lista ligada. Cada registro do arquivo de vértices tem a forma

VÉRTICE	PROX-V	PTR	

Aqui, VÉRTICE será o nome do vértice, PROX-V aponta para o próximo vértice na lista de vértices no arquivo de vértices, e PTR aponta para o primeiro elemento da lista de adjacências do vértice que aparece no arquivo de arestas. A área sombreada indica que podem existir outras informações no registro correspondente ao vértice.

(*b*) ***Arquivo de arestas*:** o arquivo de arestas contém as arestas de G e também todas as listas de adjacências de G onde cada lista é mantida na memória por uma lista ligada. Cada registro do arquivo de arestas representará uma única aresta em G e, portanto, corresponderá a um único vértice na lista de adjacências. O registro, normalmente, terá a forma

ARESTA	INI-V	TERM-V	PROX-A	

Aqui:

(1) ARESTA será o nome da aresta (se houver).

(2) INI-V aponta para a localização, no arquivo de vértices, do vértice inicial da aresta.

(3) TERM-V aponta para a localização, no arquivo de vértices, do vértice terminal (final) da aresta. As listas de adjacências aparecem neste campo.

(4) PROX-A aponta para a localização, no arquivo de arestas, do próximo vértice na lista de adjacências.

Enfatizamos que as listas de adjacências consistem nos vértices terminais e são, portanto, mantidas pelo campo TERM-V. A área sombreada indica que podem existir outras informações no registro correspondente à aresta. Notamos que a ordem dos vértices, em qualquer lista de adjacências, depende da ordem em que as arestas (pares de vértices) aparecem na entrada.

A Figura 9-12 mostra como o grafo G da Figura 9-11(*a*) pode aparecer na memória. Aqui, os vértices de G são mantidos na memória por uma lista ligada usando a variável START para apontar para o primeiro vértice (como alternativa, pode-se usar um *array* linear para lista de vértices, e então PROX-V não seria necessário). A escolha de oito posições para o arquivo de vértices e de 10 posições para o arquivo de arestas é arbitrária. O espaço adicional nos arquivos será usado se vértices ou arestas adicionais forem inseridos no grafo. A Figura 9-12 também mostra, com setas, a lista de adjacências $[B, C, D]$ do vértice A.

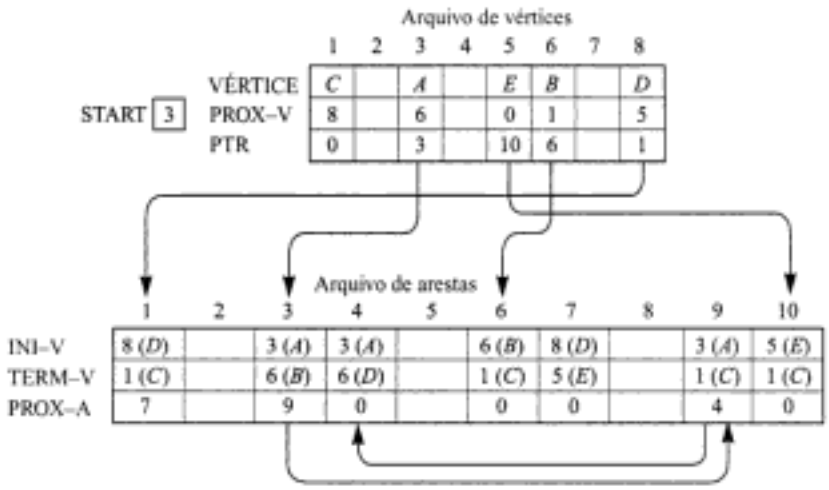


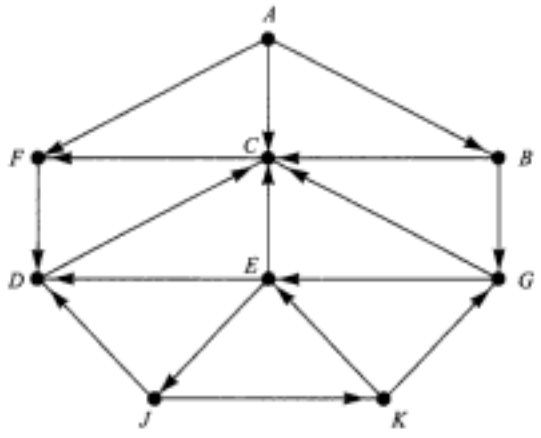
Fig. 9-12

9.8 ALGORITMOS PARA GRAFOS: BUSCAS EM PROFUNDIDADE E EM LARGURA

Esta seção discute dois algoritmos importantes em grafos para um grafo dado G. Qualquer algoritmo particular para grafos depende da maneira com que o grafo está armazenado na memória. Aqui, assumimos que G é mantido na memória através da sua estrutura de adjacências. Nosso grafo para teste, G, com sua estrutura de adjacências aparece na Figura 9-13.

Muitas aplicações de grafos requerem o exame sistemático dos vértices e arestas do grafo G. Existem duas maneiras-padrão pelas quais isto é feito. Uma maneira é chamada de *busca em profundidade* (DFS), e a outra é chamada de *busca em largura* (BFS)[†]. (Esses algoritmos são essencialmente idênticos aos seus análogos para grafos não orientados, descritos no Capítulo 8.)

[†] N. de T. As siglas DFS e BFS referem-se a, respectivamente, *depth-first search* e *breadth-first search*; foram mantidas no texto por serem de uso corrente em ciência da computação. O algoritmo BFS também é conhecido como busca em amplitude.



(a)

Listas de adjacências
A: B, C, F
B: C, G
C: F
D: C
E: J, C, D
F: D
G: C, E
J: K, D
K: G, E

(b)

Fig. 9-13

Durante a execução dos nossos algoritmos, cada vértice (nó) N de G terá um dos seguintes estados, chamados de *status* de N, como a seguir

STATUS = 1:	(estado de prontidão)	o estado inicial de um vértice N.
STATUS = 2:	(estado de espera)	o vértice N está numa lista de espera, aguardando para ser processado.
STATUS = 3:	(estado processado)	o vértice foi processado.

A lista de espera para busca em profundidade será uma PILHA (modificada), enquanto a lista de espera para a busca em largura será uma FILA.

(*a*) ***Busca em profundidade*:** A idéia geral de uma busca em profundidade começada pelo vértice A é descrita a seguir. Primeiramente processamos o vértice inicial A. Depois processamos cada vértice N ao longo de um caminho P que inicia em A; isto é, processamos um vizinho de A, depois um vizinho de um vizinho de A, e assim por diante. Depois de atingirmos um "beco sem saída", isto é, um vértice que não tem vizinhos não processados, retrocedemos então no caminho P até que possamos continuar ao longo de outro caminho P', e assim por diante. O retrocesso é feito usando uma PILHA contendo os vértices inicias de novos possíveis caminhos. Também precisamos de um campo, STATUS, que nos diz o estado corrente de qualquer vértice de tal forma que nenhum vértice seja processado mais de uma vez. O algoritmo é o seguinte.

Algoritmo 9.8A: (**Busca em profundidade**) Este algoritmo executa uma busca em profundidade em um grafo orientado G começando de um vértice de partida A.

Passo 1 Inicialize todos os vértices para o estado prontidão (STATUS = 1).

Passo 2 Insira o vértice de partida A em PILHA e mude seu *status* para estado de espera (STATUS = 2).

Passo 3 Repita os Passos 4 e 5 até que a PILHA esteja vazia.

Passo 4 Retire o vértice N do topo da PILHA. Processe N, faça STATUS(N) = 3, estado processado.

Passo 5 Examine cada vizinhança J de N.

- (*a*) Se STATUS(J) = 1(estado de prontidão), insira J na PILHA e faça STATUS(J) = 2 (estado de espera).
- (*b*) Se STATUS(J) = 2 (estado de espera), delete o J anterior da PILHA e insira o J corrente na pilha.
- (*c*) Se STATUS(J) = 3 (estado processado), ignore o vértice J.

[Fim do *loop* no Passo 3.]

Passo 6 Saia.

O algoritmo anterior irá processar apenas os vértices que são alcançáveis saindo do vértice de partida A. Suponha que se queira processar todos os vértices no grafo G. Então o algoritmo precisa ser modificado de tal forma que recomece de um novo vértice que ainda esteja no estado de prontidão (STATUS = 1). Esse novo vértice, digamos B, pode ser obtido percorrendo a lista de vértices.

Observação: A estrutura PILHA no algoritmo acima não é tecnicamente uma pilha, uma vez que, no Passo 5(b), permitimos que um vértice J seja deletado e posteriormente inserido no topo da pilha (embora seja o mesmo vértice J, representa uma aresta diferente na estrutura de adjacências). Se não movermos J no Passo 5(b), obteremos uma forma alternativa para o algoritmo.

Exemplo 9.10 Considere nosso grafo de teste G na Figura 9-13. Suponha que queremos determinar e imprimir todos os vértices alcançáveis a partir do vértice J (incluindo o próprio J). Uma maneira de fazer isso é usar o algoritmo de busca em profundidade de G começando no vértice J.

Aplicando o Algoritmo 9.8A, os vértices serão processados e impressos na seguinte ordem:

$$J,\quad K,\quad G,\quad E,\quad C,\quad F,\quad D$$

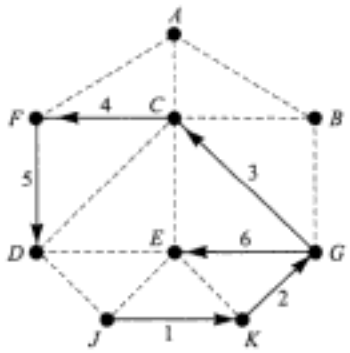
Especificamente, a Figura 9-14(a) mostra a seqüência de listas de espera em PILHA e os vértices em processamento. (A barra / indica que um vértice é deletado da lista de espera.) Enfatizamos que cada vértice, excluindo J, provém de uma lista de adjacências e, portanto, ele é o vértice terminal de uma única aresta do grafo. Indicamos a aresta rotulando o vértice terminal com o vértice inicial da aresta. Por exemplo,

$$J^D$$

significa que D está na lista de adjacências de J, e, portanto, D é o vértice terminal de uma aresta começando em J. Estas arestas formam uma árvore com raízes T tendo J como raiz, o que está representado na Figura 9-14(b). (Os números indicam a ordem em que as arestas são adicionadas à árvore T.) Essa árvore T gera o subgrafo G' de G que consiste nos vértices alcançáveis a partir de J.

Vértices	PILHA
	J
J	J^K, J^D
J^K	K^G, K^E, J^D
K^G	G^C, G^E, K^E, K^D
G^C	C^F, G^E, K^D
C^F	F^D, G^E, K^D
F^D	G^E
G^E	$\varnothing$

(a)



(b)

Fig. 9-14

(b) ***Busca em largura*:** A idéia geral por trás de uma busca em largura começando com um vértice de partida A é descrita a seguir. Primeiramente processamos o vértice de partida A. Depois, processamos todos os vizinhos de A. A seguir, os vizinhos dos vizinhos de A, e assim sucessivamente. Naturalmente precisamos ter o controle dos vizinhos de um vértice, e precisamos garantir também que nenhum vértice seja processado duas vezes. Isso é feito usando FILA para conhecer os vértices aguardando processamento, e pelo campo STATUS que nos diz o *status* corrente de um vértice. O algoritmo vem a seguir.

Algoritmo 9.8B: (**Busca em largura**) Este algoritmo executa a busca em largura em um Grafo G começando com um vértice de partida A.

Passo 1 Inicialize todos os vértices para o estado de prontidão (STATUS = 1).

Passo 2 Coloque o vértice de partida A em FILA e mude seu *status* para estado de espera (STATUS =2).

Passo 3 Repita os Passos 4 e 5 até que FILA esteja vazia.

Passo 4 Remova o vértice N na frente da FILA. Processe N, faça STATUS(N) = 3, o estado processado.

Passo 5 Examine cada vizinhança J de N.

(a) Se STATUS(J) = 1(estado de prontidão), coloque J no final de FILA e faça STATUS(J) = 2 (estado de espera).

(b) Se STATUS(J) = 2 (estado de espera), ou STATUS(J) = 3 (processado), ignore o vértice J. [Fim do *loop* no Passo 3.]

Passo 6 Saia.

Novamente, o algoritmo acima irá processar apenas os vértices que são alcançáveis a partir do vértice de partida A. Suponha que se queira processar todos os vértices no grafo G. Então o algoritmo precisa ser modificado de tal forma que recomece de um novo vértice que ainda esteja no estado de prontidão (STATUS = 1). Esse vértice B pode ser obtido percorrendo a lista de vértices.

Exemplo 9.11 Considere nosso grafo de teste G na Figura 9-13. Suponha que G representa os vôos diários entre cidades, e suponha que queremos voar de uma cidade A para uma cidade J com um número mínimo de escalas. Isto é, queremos achar o caminho mínimo de A para J (onde cada aresta tem peso 1). Uma maneira de fazer isso é usar o algoritmo de busca em largura em G começando no vértice A e parando tão logo J seja encontrado, isto é, adicionado à lista de espera.

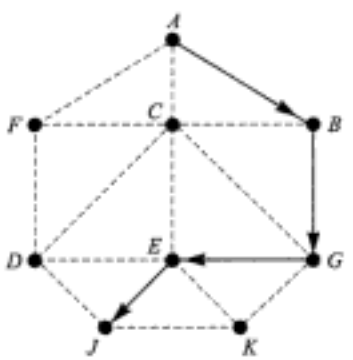
A Figura 9-15(a) mostra a seqüência de listas de espera em FILA e os vértices em processamento até que o vértice J seja encontrado. Assim, trabalhamos no sentido reverso, a partir de J, para obter o caminho desejado

$$E^J \leftarrow G^E \leftarrow B^G \leftarrow A^B \leftarrow A \qquad \text{ou} \qquad A \rightarrow B \rightarrow G \rightarrow E \rightarrow J$$

que está representado na Figura 9-15(b). Portanto, um vôo da cidade A para a cidade J fará três escalas intermediárias, em B, G e E. Note que o caminho não inclui todos os vértices processados pelo algoritmo.

Vértice	FILA
	A
A	A^B, A^C, A^F
A^F	F^D, A^B, A^C
A^C	F^D, A^B
A^B	B^G, F^D
F^D	B^G
B^G	G^E
G^E	E^J

(a)



(b)

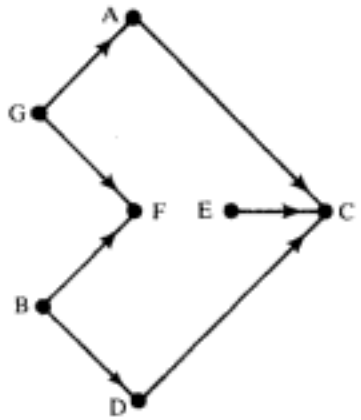
Fig. 9-15

9.9 GRAFOS ORIENTADOS ACÍCLICOS E ORDENAÇÃO TOPOLÓGICA

Seja S um grafo orientado tal que: (1) cada vértice v_i de S representa uma tarefa e que (2) cada aresta (orientada) (u, v) de S significa que a tarefa u deve ser completada antes do início da tarefa v. Suponha que um tal grafo S contém um ciclo, por exemplo

$$P = (u, v, w, u)$$

Isso significa que precisamos concluir a tarefa u antes de iniciar v, precisamos completar a tarefa v antes de iniciar w, e precisamos completar a tarefa w antes de iniciar a tarefa u. Logo, não podemos começar nenhuma das três tarefas no ciclo. Conseqüentemente, um grafo S deste tipo, representando tarefas relacionadas por pré-requisitos, não pode ter ciclos ou, em outras palavras, um grafo S deste tipo deve ser *acíclico*. Um grafo orientado acíclico é referenciado abreviadamente como um *dag*[†]. A Figura 9-16 é um exemplo deste tipo de grafo.



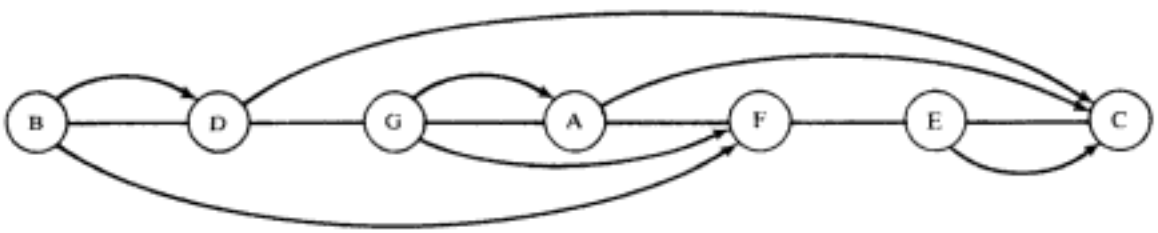
(*a*)

Listas de Adjacências	
A:	C
B:	D, F
C:	
D:	C
E:	C
F:	
G:	A, F

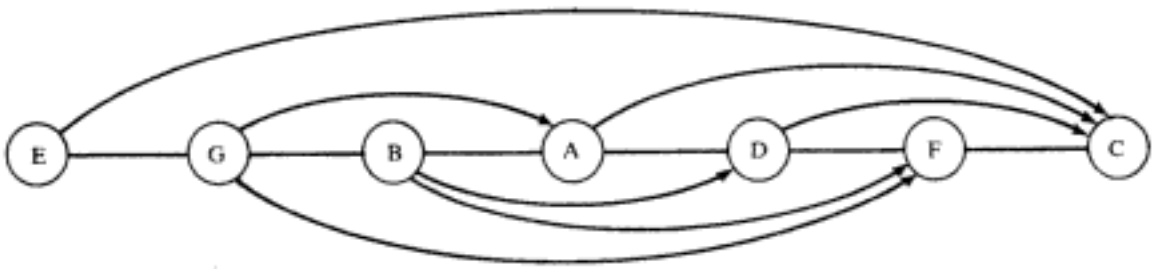
(*b*)

Fig. 9-16

Uma operação fundamental em um grafo orientado acíclico S é o processamento dos vértices, um após o outro, de tal forma que o vértice u é sempre processado antes do vértice v se (u, v) é uma aresta. Esta ordenação linear T dos vértices de S, que pode não ser única, é dita *ordenação topológica*. A Figura 9-17 mostra duas ordenações topológicas do grafo S na Figura 9-16. Incluímos as arestas de S na Figura 9-17 para mostrar que são compatíveis com a direção da ordenação linear.



(*a*)



(*b*)

Fig. 9-17 Duas ordenações topológicas.

[†] N. de T. Do inglês, *directed acyclic graph*.

Apresentamos a seguir o principal resultado teórico desta seção.

Teorema 9-8: seja S um grafo acíclico orientado finito; então, existe uma ordenação topológica T do grafo S.

Note que o teorema afirma apenas que a ordenação topológica existe. Apresentamos agora um algoritmo que irá determinar uma ordenação topológica. A idéia central do algoritmo é de que qualquer vértice (nó) N com grau de entrada zero pode ser escolhido como primeiro elemento na ordem T. Essencialmente, o algoritmo repete os dois passos seguintes até que S esteja vazio:

(1) Ache um vértice N com grau de entrada zero.
(2) Delete N e suas arestas do grafo S.

Usamos uma FILA auxiliar para guardar temporariamente todos os vértices com grau zero. Apresentamos o algoritmo a seguir.

Algoritmo 9.9: o algoritmo determina uma ordenação topológica T de um grafo orientado acíclico S.

Passo 1 Ache o o grau de entrada INDEG(N) de cada vértice N de S.

Passo 2 Insira todos os vértices de grau zero em FILA

Passo 3 Repita os Passos 4 e 5 até que FILA esteja vazia.

Passo 4 Remova e processe o primeiro vértice N de FILA.

Passo 5 Repita para cada vizinhança M do vértice N.

(a) Faça INDEG(M): = INDEG(M) –1.
[Deleta a aresta de N para M.]

(b) Se INDEG(M) = 0, adicione M na fila.
[Fim do *loop*.]
[Fim do *loop* do Passo 3.]

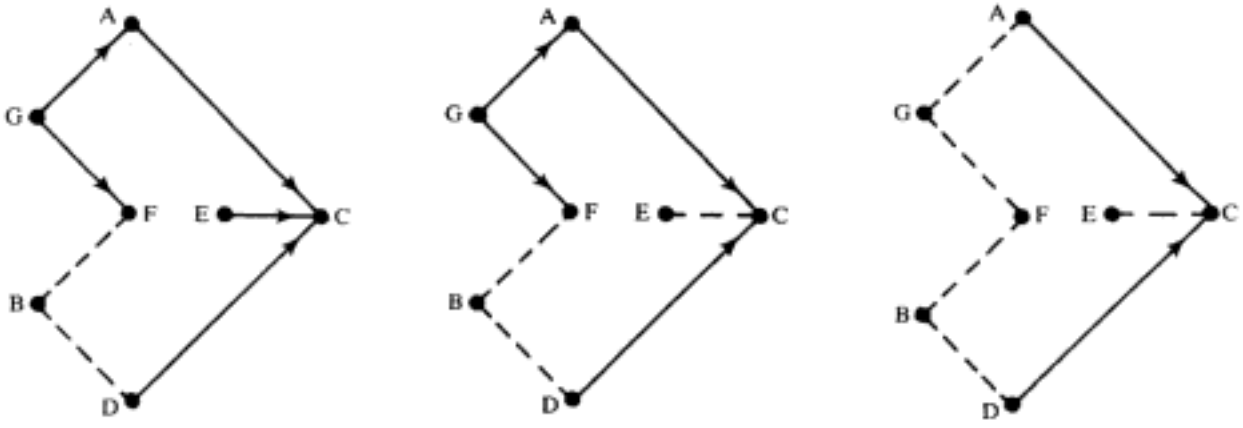
Passo 6 Saia

Exemplo 9.12 Suponha que o Algoritmo 9.9 é aplicado no grafo S da Figura 9-16. Obtemos a seguinte seqüência de elementos em FILA e seqüência de vértices em processamento:

Vértice		*B*	*E*	*G*	*D*	*A*	*F*	*C*
FILA:	*GEB*	*DGE*	*DG*	*FAD*	*FA*	*CF*	*C*	∅

A Figura 9-18 mostra o grafo S à medida que cada um dos três primeiros vértices, B, E e G, são deletados de S. A ordenação topológica T é a seqüência de vértices processados, isto é:

$$T: \quad B, E, G, D, A, F, C$$



(a) B deletado (b) E deletado. (c) G deletado.

Fig. 9-18

9.10 ALGORITMO DE PODA PARA O CAMINHO MÍNIMO

Seja G um grafo orientado ponderado acíclico. Procuramos o menor caminho entre dois vértices, por exemplo, u e w. Assumimos que G é finito e assim, a cada passo, existe um número finito de movimentos. Como G é acíclico, todos os caminhos entre u e w podem ser dados por uma árvore com raízes tendo u como raiz. A Figura 9-19(b) enumera todos os caminhos entre u e w no grafo da Figura 9-19(a).

Uma maneira de achar o caminho mínimo entre u e w é simplesmente computar o comprimento de todos os caminhos da árvore com raízes correspondente. Por outro lado, suponha que dois caminhos parciais levem para um vértice intermediário v. A partir deste vértice, precisamos considerar apenas o menor caminho parcial; isto é, podamos a árvore no vértice correspondente ao maior caminho parcial. Este algoritmo de poda[†] está descrito abaixo.

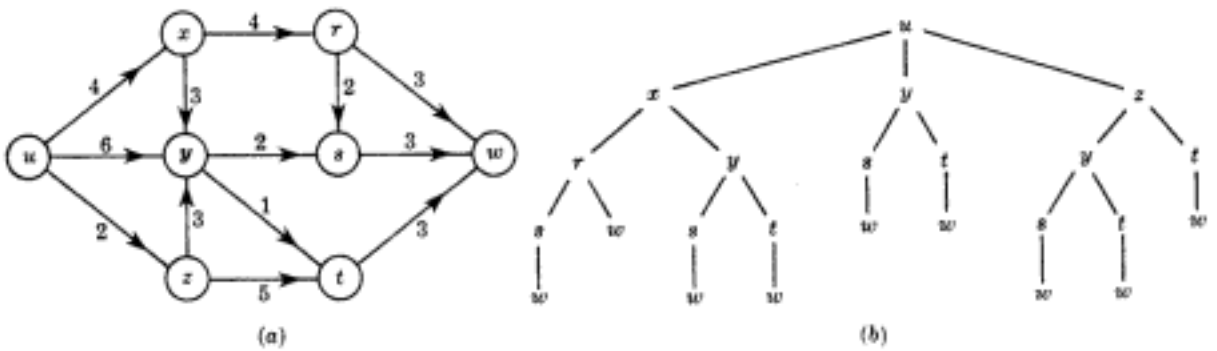


Fig. 9-19

Algoritmo de Poda

Este algoritmo determina o caminho mínimo entre um vértice u e um vértice w em um grafo orientado ponderado acíclico G. O algoritmo tem as seguintes propriedades:

(a) Durante o algoritmo, a cada vértice v' de G, são associadas duas grandezas:
  (1) um número $\ell(v')$ denotando o comprimento mínimal do caminho corrente de u para v',
  (2) um caminho $p(v')$ de u para v' de comprimento $\ell(v')$.

(b) Inicialmente, fazemos $\ell(u) = 0$ e $p(u) = u$. Para qualquer outro vértice v, é feita a atribuição inicial $\ell(v) = \infty$ e $p(v) = \varnothing$.

(c) Cada passo do algoritmo examina uma aresta $e = (v', v)$ de v' para v com, digamos, comprimento k. Calculamos $\ell(v') + k$.
  (1) Suponha que $\ell(v') + k < \ell(v)$. Então, achamos um caminho menor de u para v. Assim, atualizamos:

$$\ell(v) = \ell(v') + k \qquad \text{e} \qquad p(v) = p(v')v$$

  (Isto é sempre verdadeiro quando $\ell(v) = \infty$, isto é, quando visitamos o vértice v pela primeira vez.)
  (2) Caso contrário, $\ell(v)$ e $p(v)$ não são alterados.

  Se nenhuma outra aresta não examinada chegar a v, dizemos que $p(v)$ *foi determinado*.

(d) O algoritmo termina quando $p(w)$ é determinado.

Observação: A aresta $e = (v', v)$ em (c) só pode ser escolhida se v' tiver sido previamente visitado, isto é, se $p(v') \neq \varnothing$. Além disso, em geral é melhor examinar uma aresta que começa em um vértice v' cujo caminho $p(v')$ já foi determinado.

[†] N. de T. No original, *pruning*, nome usado, por vezes, sem tradução.

Exemplo 9.13 Aplicamos o algoritmo de poda ao grafo G da Figura 9-19(a).

A partir de u: Os vértices sucessores são x e z, que estão sendo percorridos pela primeira vez. Logo,

(1) Faça $\ell(x) = 4$, $p(x) = ux$.
(2) Faça $\ell(y) = 6$, $p(y) = uy$.
(3) Faça $\ell(z) = 2$, $p(z) = uz$.

Note que $p(x)$ e $p(z)$ foram determinados.

A partir de x: Os vértices sucessores são r, que está sendo percorrido pela primeira vez, e y. Logo,

(1) Faça $\ell(r) = 4 + 4 = 8$, e $p(r) = p(x)r = uxr$.
(2) Calculamos:

$$\ell(x) + k = 4 + 3 = 7 \text{ que não é menor do que } \ell(y) = 6.$$

Logo, não alteramos $\ell(y)$ e $p(y)$.

Note que $p(r)$ foi determinado.

A partir de z: Os vértices sucessores são t, que está sendo percorrido pela primeira vez, e y. Logo,

(1) Faça $\ell(t) = \ell(z) + k = 2 + 5 = 7$, e $p(t) = p(z)t = uzt$.
(2) Calculamos:

$$\ell(z) + k = 2 + 3 = 5 \text{ que é menor do que } \ell(y) = 6.$$

Achamos um caminho menor e, portanto, atualizamos $\ell(y)$ e $p(y)$, isto é, fazemos

$$\ell(y) = \ell(z) + k = 5 \text{ e } p(y) = p(z)y = uzy$$

Agora, $p(y)$ foi determinado.

A partir de y: Os vértices sucessores são s, que está sendo percorrido pela primeira vez, e t. Logo,

(1) Faça $\ell(s) = \ell(y) + k = 5 + 2 = 7$, e $p(s) = p(y)s = uzys$.
(2) Calculamos:

$$\ell(y) + k = 5 + 1 = 6 \text{ que é menor do que } \ell(t) = 7.$$

Assim, mudamos $\ell(t)$ e $p(t)$ para:

$$\ell(t) = \ell(y) + 1 = 6 \text{ e } p(t) = p(y)t = uzyt$$

Agora, $p(t)$ foi determinado.

A partir de r: Os vértices sucessores são w, que está sendo percorrido pela primeira vez, e s. Logo,

(1) Faça $\ell(w) = \ell(r) + 3 = 11$, e $p(w) = p(r)w = uxrw$.
(2) Calculamos:

$$\ell(r) + k = 8 + 2 = 10 \text{ que não é menor do que } \ell(s) = 7.$$

Então deixamos $\ell(s)$ e $p(s)$ inalterados.
Agora, $p(s)$ foi determinado.

A partir de s: O vértice sucessor é w. Calculamos:

$$\ell(s) + k = 7 + 3 = 10 \text{ que é menor do que } \ell(w) = 11.$$

Então atualizamos $\ell(w)$ e $p(w)$ fazendo:

$$\ell(w) = \ell(s) + 3 = 10 \text{ e } p(w) = p(s)w = uzysw.$$

A partir de t: O vértice sucessor é w. Calculamos:

$$\ell(t) + k = 6 + 3 = 9 \text{ que é menor do que } \ell(w) = 10.$$

Então atualizamos $\ell(w)$ e $p(w)$ fazendo:

$$\ell(w) = \ell(t) + 3 = 9 \text{ e } p(w) = p(t)w = uzytw$$

Agora, $p(w)$ foi determinado.

O algoritmo terminou já que $p(w)$ foi determinado. Portanto,

$$p(w) = uzytw$$

é o caminho mínimo de u para w, e $\ell(w) = 9$.

As arestas examinadas no Exemplo 9.13 formam a árvore com raízes da Figura 9-20. Esta é a árvore na Figura 9-19(*b*) que foi podada nos vértices pertencentes aos caminhos parciais maiores. Observe que apenas 13 dos 23 vértices originais da árvore foram verificados.

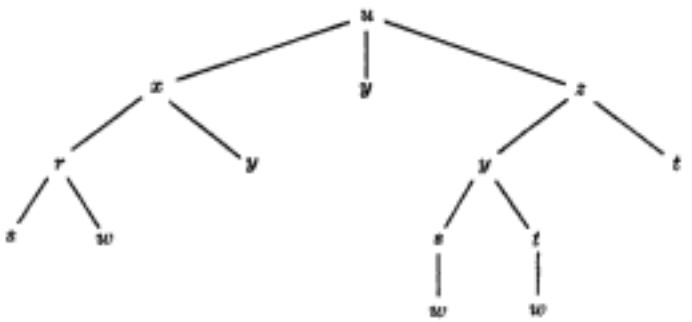


Fig. 9-20

Problemas Resolvidos

Terminologia de Grafos

9.1 Considere o grafo orientado G da Figura 9-21.

(*a*) Descreva G formalmente.

(*b*) Ache todos os caminhos simples de X para Z.

(*c*) Ache todos os caminhos simples de Y para Z.

(*d*) Ache todos os ciclos em G.

(*e*) G é unilateralmente conexo? É fortemente conexo?

(*a*) O conjunto de vértices V tem quatro vértices, e o conjunto de arestas E tem sete arestas (orientadas) como a seguir:

$$V = \{X, Y, Z, W\} \qquad \text{e} \qquad E = \{(X, Y), (X, Z), (X, W), (Y, W), (Z, Y), (Z, W), (W, Z)\}$$

(*b*) Existem três caminhos simples de X para Z, que são (X, Z), (X, W, Z) e (X, Y, W, Z).

(*c*) Existe apenas um caminho simples de Y para Z, que é (Y, W, Z).

(*d*) Existe apenas um ciclo em G, que é (Y, W, Z, Y).

(*e*) G é unilateralmente conexo, pois (X, Y, W, Z) é um caminho gerador. G não é fortemente conexo, uma vez que não existem caminhos geradores fechados.

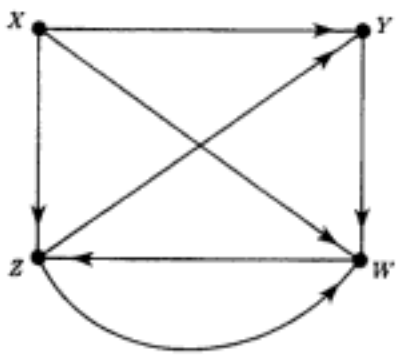


Fig. 9-21

9.2 Considere o grafo orientado G na Figura 9-21.

(*a*) Ache o grau de entrada e o grau de saída de cada vértice de G.

(*b*) Ache a lista de sucessores de cada vértice de G.

(*c*) Existem fontes ou sumidouros?

(*d*) Ache o subgrafo H de G determinado pelo conjunto de vértices $V' = \{X, Y, Z\}$.

(*a*) Conte o número de arestas terminando e começando em um vértice v para obter, respectivamente, $d^-(v)$ e $d^+(v)$. Isso produz os dados:

$$d^-(v)\,(X) = 0, \quad d^-(v)\,(Y) = 2, \quad d^-(v)\,(Z) = 2, \quad d^-(v)\,(W) = 3$$
$$d^+(v)\,(X) = 3, \quad d^+(v)\,(Y) = 1, \quad d^+(v)\,(Z) = 2, \quad d^+(v)\,(W) = 1$$

(Como esperado, a soma dos graus de entrada e a soma dos graus de saída, cada uma, é igual a 7, que é o número de arestas.)

(*b*) Adicione o vértice v à lista de sucessores suc(u) de u para cada aresta (u, v) em G. Isso produz:

$$\text{suc}\,(X) = [Y, Z, W], \quad \text{suc}\,(Y) = [W], \quad \text{suc}\,(Z) = [Y, W], \quad \text{suc}\,(W) = [Z]$$

(*c*) X é uma fonte, pois nenhuma aresta chega em X, isto é, $d^-(X) = 0$. Não existem sumidouros, já que todo vértice é o ponto inicial de uma aresta, isto é, tem grau de saída não nulo.

(*d*) Considere o conjunto E' consistindo em todas as arestas de G cujos pontos finais estejam em V'. Isto nos dá $E' = \{(X, Y), (X, Z), (Z, Y)\}$.

9.3 Considere o grafo orientado da Figura 9-22.

(*a*) Ache dois caminhos de v_1 para v_6.

$$\alpha = (v_1, v_2, v_4, v_6) \text{ é um tal caminho?}$$

(*b*) Ache todos os ciclos em G que incluem v_3.

(*c*) G é unilateralmente conexo?

(*a*) Um caminho simples é um caminho em que todos os vértices são distintos. Logo, (v_1, v_5, v_6) e $(v_1, v_2, v_3, v_5, v_6)$ são dois caminhos simples de v_1 para v_6. A seqüência α não é nem mesmo um caminho, já que a aresta unindo v_4 a v_6 não inicia em v_4.

(*b*) Existem dois ciclos: (v_3, v_1, v_2, v_3) e $(v_3, v_5, v_6, v_1, v_2, v_3)$.

(*c*) G é unilateralmente conexo, pois $(v_1, v_2, v_3, v_5, v_6, v_4)$ é um caminho gerador. G não é fortemente conexo, já que não existe caminho gerador fechado.

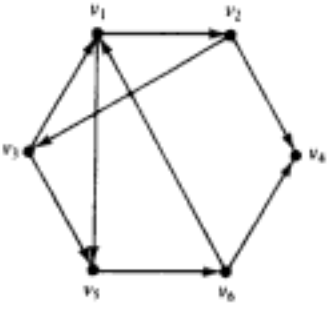


Fig. 9-22

9.4 Considere o grafo orientado da Figura 9-22.

(*a*) Ache a lista de sucessores de cada vértice de G.

(*b*) Existem fontes em G? Algum sumidouro?

(*a*) Adicione o vértice v à lista de sucessores de u, suc(u), para cada aresta (u, v) em G. Isso nos dá:

$$\text{suc}\,(v_1) = [v_2, v_5], \quad \text{suc}\,(v_2) = [v_3, v_4], \quad \text{suc}\,(v_3) = [v_1, v_5]$$
$$\text{suc}\,(v_4) = \varnothing, \quad \text{suc}\,(v_5) = [v_6], \quad \text{suc}\,(v_6) = [v_1, v_4]$$

(Como esperado, o número de sucessores é igual a 9, que é o número de arestas.)

(*b*) Não existem fontes, uma vez que todo vértice é o ponto final de alguma aresta. Apenas v_4 é um sumidouro, pois nenhuma aresta inicia em v_4, isto é, $\text{suc}\,(v_4) = \varnothing$, o conjunto vazio.

9.5 Considere o seguinte grafo orientado G:

$$V(G) = \{a, b, c, d, e, f, g\}$$

$$E(G) = \{(a,a), (b,e), (a,e), (e,b), (g,c), (a,e), (d,f), (d,b), (g,g)\}$$

(*a*) Identifique todos os laços e arestas paralelas.

(*b*) Existem fontes em G?

(*c*) Existem sumidouros em G?

(*d*) Ache o subgrafo H de G determinado pelo conjunto de vértices $V' = \{a, b, c, d\}$.

(*a*) Um laço é uma aresta com pontos inicial e final iguais. Portanto, (a, a) e (g, g) são laços. Duas arestas são paralela se elas têm os mesmos pontos inicial e final. Então, (a, e) e (a, e) são arestas paralelas.

(*b*) O vértice d é uma fonte, já que nenhuma aresta termina em d, isto é, d não aparece como segundo elemento em n nhuma aresta. Não existem outras fontes.

(*c*) Ambos, c e f, são sumidouros, pois nenhuma aresta começa em c ou f, isto é, nem c nem f aparecem como primeir elemento em qualquer aresta. Não existem outros sumidouros.

(*d*) Seja E' o conjunto de todas as arestas de G com pontos finais em $V' = \{a, b, c, d\}$. Isso nos dá $E' = \{(a, a), (d, b)$ Então $H = H(V', E')$.

9.6 Seja G o grafo orientado com vértices $V(G) = \{a, b, c, d, e\}$, e considere a seguinte lista de sucessores:

$$\text{suc}(a) = [b, c], \qquad \text{suc}(b) = \varnothing, \qquad \text{suc}(c) = [d, e]$$

$$\text{suc}(d) = [a, b, e], \qquad \text{suc}(e) = \varnothing$$

(*a*) Liste as arestas de G. (G é determinado pela sua lista de sucessores?)

(*b*) G é fracamente conexo? Unilateralmente conexo?

(*a*) Desenhe uma aresta (x, y) sempre que $y \in \text{suc}(x)$. Isso dá:

$$E(G) = \{(a,b), (a,c), (c,d), (c,e), (d,a), (d,b), (d,e)\}$$

(*b*) Como b e e são sumidouros, não existe caminho de b para e ou de e para b. Logo, G não é nem unilateralmente ne fortemente conexo. Entretanto, G é fracamente conexo, já que (c, a, b, d, e) é um semicaminho gerador.

Árvores com Raízes e Árvores Ordenadas com Raízes

9.7 Considere a árvore com raízes T da Figura 9-23.

(*a*) Identifique o caminho α da raiz R para cada um dos vértices seguintes e ache o número de nível n do vért ce: (i) H; (ii) F; (iii) M.

(*b*) Ache os irmãos[†] de E.

(*c*) Ache as folhas de T.

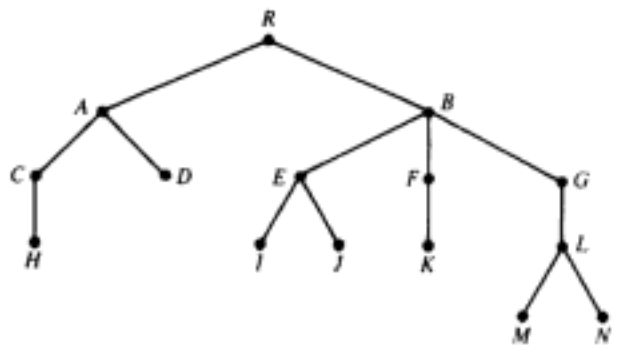


Fig. 9-23

[†] N. de T. No original, *siblings*.

(*a*) Liste os vértices no precurso ao longo da árvore a partir de R na direção dos vértices. O número de vértices diferentes de R é o número de nível.

(i) $\alpha = (R, A, C, H)$, $n = 3$; (ii) $\alpha = (R, B, F)$, $n = 2$; (iii) $\alpha = (R, B, G, L, M)$, $n = 4$.

(*b*) Os irmãos de E são F e G, já que têm o mesmo pai B.

(*c*) As folhas são vértices sem filhos, isto é, H, D, I, J, K, M, N.

9.8 Considere a seguinte situação, típica no mundo dos negócios. Uma companhia que vende seus produtos em duas grandes regiões geográficas está planejando introduzir um novo produto. O procedimento normal para introdução de produtos é descrito a seguir. Primeiramente, o produto é introduzido em uma região de teste de mercado bem pequena na região I. Se fracassar, é descontinuado; se for bem-sucedido, é introduzido na região I. Se o produto for um sucesso na região I, é introduzido em toda a região II, se não, é introduzido em um pequeno mercado de teste na região II. De novo, se for bem-sucedido, é introduzido em toda a região. Use uma árvore para identificar todas as possibilidades para a introdução do produto.

As possibilidades são descritas pela árvore na Figura 9-24. Existem quatro possibilidades, como indicado pelos quatro ramos a partir da raiz até as folhas da árvore (onde a raiz, agora, está à esquerda da árvore):

(1) O produto não tem sucesso na primeira região pequena para teste de mercado da região I e é descontinuado.

(2) O produto é bem recebido na primeira região pequena para teste de mercado, é bem recebido na região I, e é introduzido na região II.

(3) O produto é bem recebido na primeira região pequena para teste de mercado, mas não é bem recebido na região I. É testado em um pequeno mercado de teste na região II, não é bem sucedido e é descontinuado.

(4) O produto é bem-sucedido no primeiro mercado de teste pequeno mas não é bem recebido na região I. É testado em um pequeno mercado na região II, é bem recebido e é introduzido nesta região.

Fig. 9-24

9.9 A Figura 9-25 mostra uma árvore ordenada com raízes T cujos vértices são rotulados usando o sistema de endereçamento universal. Ache a ordem lexicográfica dos endereços da árvore T.

Como uma árvore ordenada com raízes T é normalmente desenhada de tal modo que as arestas são ordenadas da esquerda para a direita, como na Figura 9-25, a ordem lexicográfica pode ser obtida lendo verticalmente o ramo mais à esquerda, depois o segundo ramo da esquerda, e assim por diante. Conseqüentemente, lendo o ramo da extrema esquerda de cima para baixo, obtemos:

$$0, \quad 1, \quad 1.1, \quad 1.1.1$$

O próximo ramo é 1.2; assim, inserimos 1.2 na lista para obter

$$0, \quad 1, \quad 1.1, \quad 1.1.1, \quad 1.2$$

Analogamente, o próximo ramo acrescenta

$$1.3, \quad 1.3.1, \quad 1.3.1.1$$

à nossa lista. Procedendo desta maneira, obtemos:

$$0, \quad 1, \quad 1.1, \quad 1.1.1, \quad 1.2, \quad 1.3, \quad 1.3.1, \quad 1.3.1.1, \quad 1.3.2, \quad 2, \quad 2.1, \quad 2.2, \quad 2.2.1.$$

Fig. 9-25

9.10 Considere os seguintes endereços que estão em ordem aleatória:

$$1, \quad 2.2.1, \quad 3.2, \quad 2.2.1.1, \quad 1.1.1, \quad 0, \quad 2.1, \quad 3.2.1.1,$$
$$3, \quad 3.1, \quad 2.2, \quad 2.1.1, \quad 3.2.1, \quad 1.1, \quad 3.2.1.2, \quad 2, \quad 1.1.2$$

(*a*) Coloque os endereços em ordem lexicográfica.

(*b*) Desenhe a árvore ordenada com raízes correspondente.

(*a*) A ordem lexicográfica dos endereços é a seguinte:

$$0, \quad 1, \quad 1.1, \quad 1.1.1, \quad 1.1.2, \quad 2, \quad 2.1, \quad 2.1.1, \quad 2.2, \quad 2.2.1,$$
$$2.2.1.1, \quad 3, \quad 3.1, \quad 3.2 \quad 3.2.1, \quad 3.2.1.1, \quad 3.2.1.2$$

(*b*) Para desenhar a árvore *T*, associada com a ordem lexicográfica dada, inicie com o ramo mais à esquerda, depois adicione o ramo mais próximo, e assim por diante. Depois desenhe a raiz 0, ramificando para 1, ramificando para 1.1, e depois para 1.1.1. Como 2 não é sucessor de 1.1.1 na árvore, é o início do ramo seguinte, que é 2, 2.1, 2.1.1. Continuando desta forma, obtêm-se a árvore da Figura 9-26.

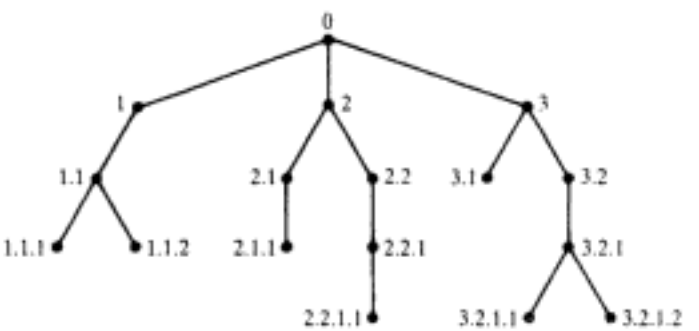


Fig. 9-26

Representação Seqüencial de Grafos

9.11 Considere o grafo G da Figura 9-21. Suponha que os vértices estão armazenados na memória em um *array* DATA como a segir:

$$\text{DATA: } X,\ Y,\ Z,\ W$$

(*a*) Ache a matriz de adjacências A do grafo G.

(*b*) Ache a matriz de caminhos P de G usando potências da matriz de adjacências A.

(*c*) G é fortemente conexo?

(*a*) Os vértices (nós) são ordenados, normalmente, de acordo com a maneira com que aparecem na memória; isto é, assumimos $v_1 = X$, $v_2 = Y$, $v_3 = Z$, $v_4 = W$. A matriz de adjacências A de G é:

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Aqui, $a_{ij} = 1$ se existe uma aresta de v_i para v_j; caso contrário, $a_{ij} = 0$.

(*b*) Como G tem quatro vértices, compute A^2, A^3, A^4, e $B_4 = A + A^2 + A^3 + A^4$:

$$A^2 = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \qquad A^3 = \begin{pmatrix} 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 0 & 2 & 2 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad B_4 = \begin{pmatrix} 0 & 5 & 6 & 8 \\ 0 & 1 & 2 & 3 \\ 0 & 3 & 3 & 5 \\ 0 & 2 & 3 & 5 \end{pmatrix}$$

A matriz de caminhos P é então obtida fazendo $p_{ij} = 1$ sempre que ocorre um elemento não nulo na matriz B_4.

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

(*c*) A matriz de caminhos mostra que não existe caminho de v_2 para v_1. De fato, não existe caminho de nenhum nó para v_1. Portanto, G não é fortemente conexo.

9.12 Considere a matriz de adjacências A do grafo G da Figura 9-21 obtida no Problema 9.11. Ache a matriz de caminhos P de G usando o algoritmo de Warshall em vez das potências de A.

Compute as matrizes P_0, P_1, P_2, P_3 e P_4, onde inicialmente $P_0 = A$ e

$$P_k[i,j] = P_{k-1}[i,j] \vee (P_{k-1}[i,j] \wedge P_{k-1}[k,j])$$

Isto é,

$$P_k[i,j] = 1 \quad \text{se} \quad P_{k-1}[i,j] = 1 \quad \text{ou ambos} \quad P_{k-1}[i,k] = 1 \quad \text{e} \quad P_{k-1}[k,j] = 1$$

Então:

$$P_1 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad P_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad P_4 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Observe que $P_0 = P_1 = P_2 = A$. As mudanças em P_3 ocorrem pelas seguintes razões:

$$P_3(4,2) = 1 \quad \text{porque} \quad P_2(4,3) = 1 \quad \text{e} \quad P_2(3,2) = 1$$
$$P_3(4,4) = 1 \quad \text{porque} \quad P_2(4,3) = 1 \quad \text{e} \quad P_2(3,4) = 1$$

As mudanças em P_4 ocorrem de modo análogo. A matriz P_4 é a matriz de caminhos requerida para o grafo G.

9.13 Desenhe uma representação gráfica de um grafo ponderado G que é mantido na memória pelo *array* de vértices DATA, descrito a seguir, e a matriz de pesos W:

$$\text{DATA: } X,\ Y,\ S,\ T; \qquad W = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 5 & 0 & 1 & 7 \\ 2 & 0 & 0 & 4 \\ 0 & 6 & 8 & 0 \end{bmatrix}$$

O gráfico aparece na Figura 9-27. Os vértices são rotulados pelos elementos em DATA. Além disso, se $w_{ij} \neq 0$, existe uma aresta de v_i para v_j com peso w_{ij}. (Assumimos $v_1 = X, v_2 = Y, v_3 = S, v_4 = T$, que é a ordem em que os vértices aparecem em DATA.)

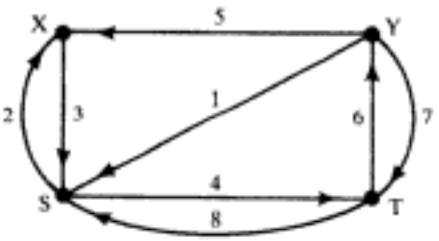


Fig. 9-27

9.14 Prove a Proposição 9.4: seja A a matriz de adjacências de um grafo G. Então, $a_K(i,j)$, o elemento na posição ij da matriz A^K, informa o número de caminhos de comprimento K de v_i para v_j.

A demonstração é feita por indução sobre K. Note primeiramente que um caminho de comprimento 1 de v_i para v_j é precisamente uma aresta (v_i, v_j). Pela definição da matriz de adjacências A, $a_1(i,j) = a_{ij}$ é o número de arestas de v_i para v_j. Portanto, a proposição é verdadeira para $K = 1$.

Suponha $K > 1$. (Assuma que G tem m nós.) Como $A^K = A^{K-1}A$,

$$a_K(i,j) = \sum_{s=1}^{m} a_{K-1}(i,s)a_1(s,j)$$

Por indução, $a_{K-1}(i,s)$ dá o número de caminhos de comprimento $K-1$ de v_i para v_s, e $a_1(s,j)$ dá o número de caminhos de comprimento 1 de v_s para v_j. Portanto, $a_{K-1}(i,s)a_1(s,j)$ dá o número de caminhos de comprimento K de v_i para v_j, onde v_s é o penúltimo nó. Logo, todos os caminhos de comprimento K de v_i para v_j podem ser obtidos somando $a_{K-1}(i,s)a_1(s,j)$ para todo s. Isto é, $a_K(i,j)$ é o número de caminhos de comprimento K de v_i para v_j. Assim, a proposição está provada.

Representação Ligada de Grafos

9.15 Um grafo ponderado G com seis vértices $A, B, \ldots, F$ está armazenado na memória usando uma representação ligada com um arquivo de vértices e um arquivo de arestas como na Figura 9-28.

(*a*) Liste os vértices na ordem em que eles aparecem na memória.

(*b*) Ache a lista de sucessores suc(v) da cada vértice v.

Arquivo de vértices

START 3

	1	2	3	4	5	6	7	8
VÉRTICE	*D*		*B*	*F*	*A*		*C*	*E*
PROX – V	7		1	5	0		8	4
PTR	9		3	0	6		10	1

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
INI-V	8	5	3		5	5	3		1	7
TERM-V	1	4	7		3	1	1		8	8
PROX-A	0	5	7		0	2	0		0	0
PESO	3	4	2		6	3	1		2	5

Fig. 9-28

(*a*) Como START = 3, a lista começa com o vértice B. Depois, PROX-V nos manda para 1(D), depois 7(C), depois 8(E), depois 4(F), e então 5(A); isto é,

$$B, \quad D, \quad C, \quad E, \quad F, \quad A$$

(*b*) Aqui, suc(A) =[1(D), 4(F), 3(B)] = [D, F, B]. Especificamente, PTR[5(A)] = 6 e TERM-V[6] = 1(d) nos diz que suc(A) começa com D. Depois, PROX-A[6] = 2 e TERM-V[2] = 4(F) nos diz que F é o próximo vértice em suc(A). Depois, PROX-A[2] = 5 e TERM-V[5] = 3(B) nos diz que B é o próximo vértice em suc(A). Entretanto, PROX-A[5] = 0 nos diz que não existem mais sucessores de A. Analogamente,

$$\text{suc}\,(B) = [C, D], \qquad \text{suc}\,(C) = [E], \qquad \text{suc}\,(D) = E, \qquad \text{suc}\,(E) = [D]$$

Ademais, suc(F) = ∅, já que PTR[4(F)]. Em outras palavras,

$$G \quad = \quad [A{:}D, F, B; \quad B{:}C, D; \quad C{:}E; \quad D{:}E; \quad E{:}D; \quad F{:}\varnothing]$$

9.16 Considere o grafo ponderado G cuja representação ligada aparece na Figura 9-28. Desenhe o gráfico de G.

Use a lista de sucessores obtida no Problema 9-16(*b*) e os pesos das arestas no arquivo de arestas na Figura 9-28 para desenhar o gráfico de G da Figura 9-29.

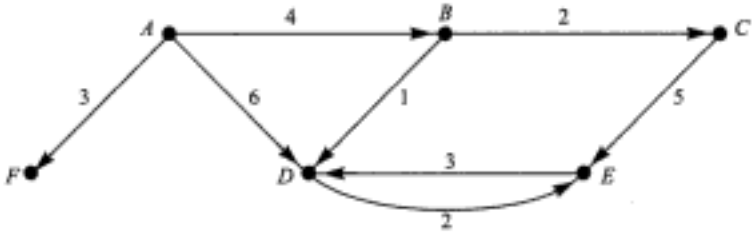


Fig. 9-29

9.17 Suponha que um grafo G seja dado pela seguinte tabela:

$$G = [X{:}Y, Z, W; \quad Y{:}X, Y, W; \quad Z{:}Z, W; \quad W{:}Z]$$

(*a*) Ache o número de vértices e arestas em G.

(*b*) Existem fontes ou sumidouros?

(*c*) Desenhe o gráfico de G.

Hidden page

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
NUM	103	106	201	203	204	301	305	308	402	
ORIG	1	5	2	2	4	4	3	6	7	
DEST	5	1	3	4	2	7	6	2	3	
PROX-A	0	0	4	0	6	0	0	0	0	

Fig. 9-32 (2 de 2)

9.20 Claramente, os dados no Problema 9.18 podem ser armazenados eficientemente em um arquivo no qual cada registro contém apenas três campos:

Número do vôo, Cidade de origem, Cidade de destino

Entretanto, se existirem muitos, muitos vôos, uma representação como esta não vai responder facilmente às seguintes perguntas usuais:

(i) Existe um vôo direto da cidade X para a cidade Y?

(ii) Pode-se voar da cidade X para a cidade Y?

(iii) Qual é a rota mais direta (menor número de escalas) da cidade X para a cidade Y?

Mostre como a resposta, por exemplo, a de (ii), pode ficar mais facilmente disponível se os dados forem armazenados na memória usando a representação ligada de um grafo como na Figura 9-32.

Uma maneira de responder (ii) é usar um algoritmo de busca em largura ou em profundidade para decidir se a cidade Y é alcançável a partir da cidade X. Esses algoritmos requerem listas de adjacências que podem ser obtidas facilmente a partir da representação ligada do grafo, mas não da representação acima, que usa apenas três campos.

Problemas Variados

9.21 Desenhe o multigrafo G correspondente à matriz de adjacências seguinte, cujos elementos são inteiros não negativos.

$$A = \begin{bmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Como A é uma matriz 4×4, G tem quatro vértices, v_1, v_2, v_3, v_4. Para cada elemento a_{ij}, desenhe a_{ij} arcos (arestas orientadas) do vértice v_i para o vértice v_j para obter o grafo da Figura 9-33.

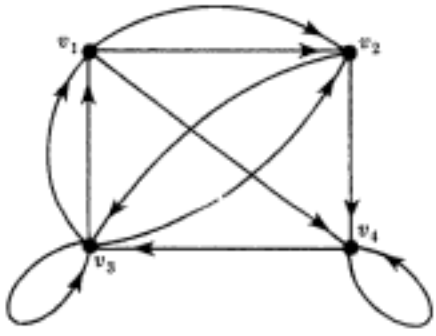


Fig. 9-33

9.22 Considere o grafo orientado acíclico S da Figura 9-34. Ache todas as possíveis ordenações topológicas de S.

Existem quatro possíveis ordenações topológicas de S. Especificamente, cada ordenação T deve iniciar com a ou b, terminar com e ou f, e c e d devem ser, respectivamente, o terceiro e quarto elementos. As quatro ordenações são:

$$T_1 = [a, b, c, d, e, f], \qquad T_2 = [b, a, c, d, e, f]$$
$$T_3 = [a, b, c, d, f, e], \qquad T_4 = [b, a, c, d, f, e]$$

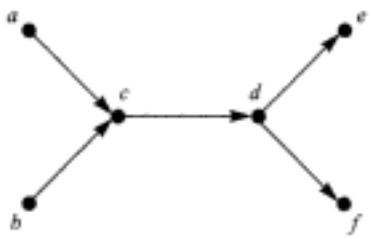


Fig. 9-34

Problemas Complementares

Terminologia de Grafos

9.23 Considere o grafo G da Figura 9-35.

(*a*) Ache o grau de entrada e o grau de saída de cada vértice.

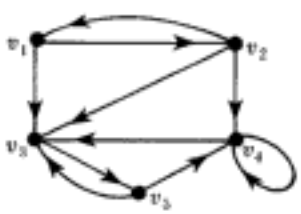
(*b*) Existem fontes ou sumidouros?

(*c*) Ache todos os caminhos de v_1 para v_4.

(*d*) Ache todos os ciclos em G.

(*e*) Ache todos os caminhos de comprimento menor ou igual a 3 de v_1 para v_3.

(*f*) G é unilateralmente conexo? Fortemente conexo?



Flig. 9-35

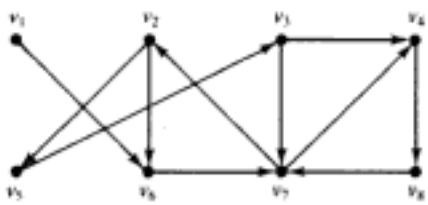


Fig. 9-36

9.24 Considere o grafo G da Figura 9-36.

(*a*) Existem fontes ou sumidouros?

(*b*) Ache todos os caminhos de v_1 para v_4.

(*c*) Ache um caminho que não seja simples de v_1 para v_4.

(*d*) Ache todos os ciclos em G que incluem v_4.

9.25 Considere o grafo G na Figura 9-36.

(*a*) Ache suc(v_1), suc (v_3), suc (v_5), suc (v_7).

(*b*) Ache um subgrafo H de G gerado por: (i) $\{v_1, v_3, v_5, v_6\}$; (ii) $\{v_2, v_3, v_6, v_7\}$.

Hidden page

Hidden page

Hidden page

9.44 Repita o Problema 9-43 para a tabela:

$$G = [A{:}D;\quad B{:}C;\quad C{:}E;\quad D{:}B, D, E;\quad E{:}A]$$

9.45 Repita o Problema 9-43 para a tabela:

$$G = [A{:}B, C, D, F;\quad B{:}E;\quad C{:}\varnothing;\quad D{:}\varnothing;\quad E{:}B, D, G;\quad F{:}D, G;\quad G{:}D]$$

9.46 Suponha que a Friendly Airways tenha oito vôos diários atendendo às sete cidades Atlanta, Boston, Chicago, Denver, Houston, Filadélfia e Washington. Suponha que os dados sobre os vôos estejam guardados na memória como na Figura 9-44, isto é, usando uma representação ligada onde as cidades e vôos aparecem em um *array* linear ordenado. Desenhe um grafo orientado rotulado G descrevendo os dados.

Arquivo de vértices

	1	2	3	4	5	6	7	8
CID	*A*	*B*	*C*	*D*	*H*	*F*	*W*	
PTR	1	2	3	8	9	5	7	

Arquivo de arestas

	1	2	3	4	5	6	7	8	9	10
NUM	101	102	201	202	203	301	302	401	402	
ORIG	1	2	3	1	6	6	7	4	5	
DEST	2	3	6	7	3	1	6	5	4	
PROX-A	4	0	0	0	6	0	0	0	0	

Fig. 9-44

9.47 Usando os dados na Figura 9-44, escreva uma rotina com dados de entrada CID X e CID Y que acha o número do vôo direto da cidade X para a cidade Y, se existir. Teste a rotina usando como dados:

(*a*) X = Atlanta, Y = Filadélfia; (*b*) X = Filadélfia, Y = Atlanta; (*c*) X = Houston, Y = Chicago; (*d*) X = Washington, Y = Chicago.

9.48 Usando os dados na Figura 9-44, escreva uma rotina com dados de entrada CID X e CID Y que acha a rota mais direta (menor número de escalas) da cidade X para a cidade Y, se existir. Teste a rotina usando os dados do Problema 9.47.

Problemas Variados

9.49 Use o algoritmo de poda para achar o menor caminho de s para t na Figura 9-45.

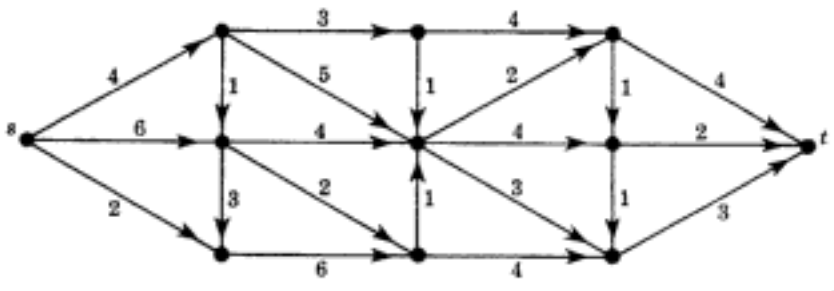


Fig. 9-45

9.50 Ache uma ordenação topológica T de cada um dos seguintes grafos:

(*a*) $G = [A{:}Z;\quad B{:}T;\quad C{:}B;\quad D{:}\varnothing;\quad X{:}D;\quad Y{:}X;\quad Z{:}B, X;\quad S{:}C, Z;\quad T{:}\varnothing]$

(*b*) $G = [A{:}X, Z;\quad B{:}A;\quad C{:}S, T;\quad D{:}Y;\quad X{:}S, T;\quad Y{:}B;\quad Z{:}\varnothing;\quad S{:}Y;\quad T{:}\varnothing]$

(*c*) $G = [A{:}C, S;\quad B{:}T, Z;\quad C{:}\varnothing;\quad D{:}Z;\quad X{:}A;\quad Y{:}A;\quad Z{:}X, Y;\quad S{:}\varnothing;\quad T{:}Y]$

Hidden page

9.34 (*a*) $A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$.

(*b*) 0, 2, 1, 0, 0...

(*c*) Fracamente e unilateralmente.

9.35 (*a*) $A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$.

(*b*) 0, 1, 1, 1...

(*c*) Fracamente e unilateralmente.

9.36 Seja $P = [p_{ij}]$. Para $i \neq j$, temos: (*a*) $p_{i,j} \neq 0$; (*b*) ou $p_{i,j} \neq 0$, ou $p_{j,i} \neq 0$.

9.37 (*a*) $A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

(*b*) (X, Z, Y, X).

(*c*) Unilateralmente.

9.38 (*a*) $A = \begin{bmatrix} 0 & 7 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 0 & 0 & 5 \\ 6 & 1 & 4 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} XYX & XY & XYS & XYST \\ YX & YSTY & YS & YST \\ STYX & STY & STYS & ST \\ TX & TY & TYS & TYST \end{bmatrix}$

9.39 (i) $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

(ii) $A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$; $P = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

9.40 (i) $W = \begin{bmatrix} 7 & 5 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 3 & 0 & 0 \\ 4 & 0 & 1 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} AA & AB & ABCD & ABD \\ BDA & BDCB & BDC & BD \\ CBDA & CB & CBDC & CBD \\ DA & DCB & DC & DCBD \end{bmatrix}$ onde

A, B, C, D são os vértices.

(ii) $W = \begin{bmatrix} 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 & 3 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 4 & 0 \end{bmatrix}$; $Q = \begin{bmatrix} ACDA & ACEB & AC & ACD & ACE \\ BDA & BDACEB & BDAC & BD & BDACE \\ CDA & CEB & CDAC & CD & CE \\ DA & DACEB & DAC & DACD & DACEB \\ EDA & EB & EDAC & ED & EDACE \end{bmatrix}$ onde

A, B, C, D, E são os vértices.

Hidden page

Capítulo 10

Árvores Binárias

10.1 INTRODUÇÃO

A árvore binária é uma estrutura fundamental em matemática e ciência da computação. Uma parte da terminologia usada para árvores com raízes, como, por exemplo, aresta, caminho, ramo, folha, profundidade e número de nível, também será usada para árvores binárias. Entretanto, usaremos o termo "nó" no lugar de "vértice" para árvores binárias. Enfatizamos que uma árvore binária não é um caso especial de árvore com raiz; são objetos matemáticos diferentes.

10.2 ÁRVORES BINÁRIAS

Uma *árvore binária* T é definida como um conjunto finito de elementos, denominados *nós*, tais que:

(1) T é vazio (chamado *árvore nula* ou *árvore vazia*) ou
(2) T contém um nó diferenciado R, denominado a *raiz* de T, e os outros nós de T formam um par ordenado de árvores binárias disjuntas T_1 e T_2.

Se T contém uma raiz R, as duas árvores T_1 e T_2 são chamadas, respectivamente, de *subárvores esquerda* e *direita* de R. Se T_1 é não vazia, então sua raiz é chamada de *sucessora esquerda* de R; analogamente, se T_2 é não vazia, sua raiz é dita *sucessora direita* de R.

A definição acima de uma árvore binária é recursiva, pois T é definida em termos de subárvores binárias T_1 e T_2. Isto quer dizer, em particular, que todo nó N de T contém uma subárvore direita e uma subárvore esquerda, podendo, cada uma delas ou ambas, serem vazias. Logo, todo nó N em T tem zero, um ou dois sucessores. Um nó sem sucessores é dito um *nó terminal*. Portanto, as duas subárvores de um nó terminal são vazias.

Representação Gráfica de uma Árvore Binária

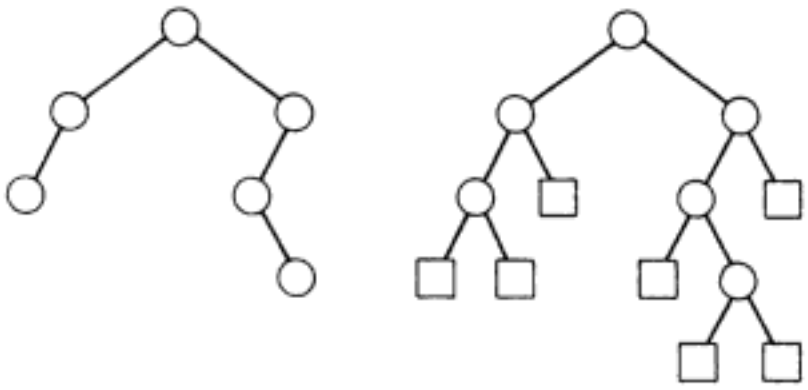
Uma árvore binária T é freqüentemente representada por um diagrama chamado de *representação gráfica* de T. Especificamente, o diagrama da Figura 10-1 representa uma árvore binária com as seguintes propriedades:

(i) T consiste em 11 nós, representados pelas letras A a L, excluído I.
(ii) A raiz de T é o nó A, no topo de diagrama.
(iii) Uma linha descendente a partir de um nó N, inclinada para a esquerda, indica um sucessor à esquerda de N; uma linha descendente a partir de um nó N, inclinada para a direita, indica um sucessor à direita de N.

Hidden page

Hidden page

Hidden page



(*a*) Árvore binária T (*b*) 2-árvore estendida

Fig.10-5 Conversão de uma árvore binária T em uma árvore estendida.

10.4 REPRESENTAÇÃO DE ÁRVORES BINÁRIAS NA MEMÓRIA

Seja T uma árvore binária. Esta seção discute duas maneiras de representar T na memória. A primeira, e mais comum, é chamada de representação ligada de T e é análoga à maneira pela qual as listas ligadas são representadas na memória. A segunda maneira, que utiliza um único *array*, é chamada de representação seqüencial de T. O requisito principal de qualquer representação de T é de que é necessário ter acesso direto à raiz R de T e, também, dado qualquer nó N de T, é preciso ter acesso direto aos filhos de N.

Representação Ligada de Árvores Binárias

Considere uma árvore binária T. A menos que especificação em contrário seja feita ou esteja implícita, T será guardada na memória por meio de uma *representação ligada* que usa três *arrays* paralelos, INFO, ESQ e DIR, e um ponteiro RAIZ, como descrito a seguir. Primeiramente, cada nó N de T corresponderá a uma posição K tal que:

(1) INFO[K] contém os dados no nó N.
(2) ESQ[K] contém a posição do filho esquerdo do nó N.
(3) DIR[K] contém a posição do filho direito do nó N.

Além disso, RAIZ contém a posição da raiz R de T. Se alguma subárvore estiver vazia, o ponteiro correspondente conterá o valor nulo; se a própria árvore T estiver vazia, RAIZ conterá o valor nulo.

Observação 1: A maioria dos nossos exemplos mostrará um único item de informação em cada nó N de uma árvore T. Em aplicações práticas, um registro inteiro pode ser armazenado no nó N. Em outras palavras, INFO pode ser, de fato, um *array* linear de registros ou uma coleção de *arrays* paralelos.

Observação 2: Qualquer endereço inválido pode ser escolhido para ponteiro nulo, denotado por NUL. Na prática, 0 ou números negativos são usados para NUL.

Exemplo 10.2 Considere a árvore binária T da Figura 10-1. Um diagrama esquemático de uma representação ligada de T aparece na Figura 10-6. Observe que cada nó está desenhado com três campos, e as subárvores vazias são desenhadas usando × para elementos nulos. A Figura 10-7 mostra como esta representação ligada de T pode aparecer na memória, onde usamos *arrays* verticais em vez de horizontais por conveniência de notação. Note que RAIZ = 5, aponta para INFO[5] = A, já que A é a raiz de T. Além disso, note que ESQ[5] = 10 aponta para INFO[10] = B já que B é o filho esquerdo de A, e DIR[5] = 2 aponta para INFO[2] = C, já que C é o filho direito de A. A escolha de 18 elementos para os *arrays* é arbitrária.

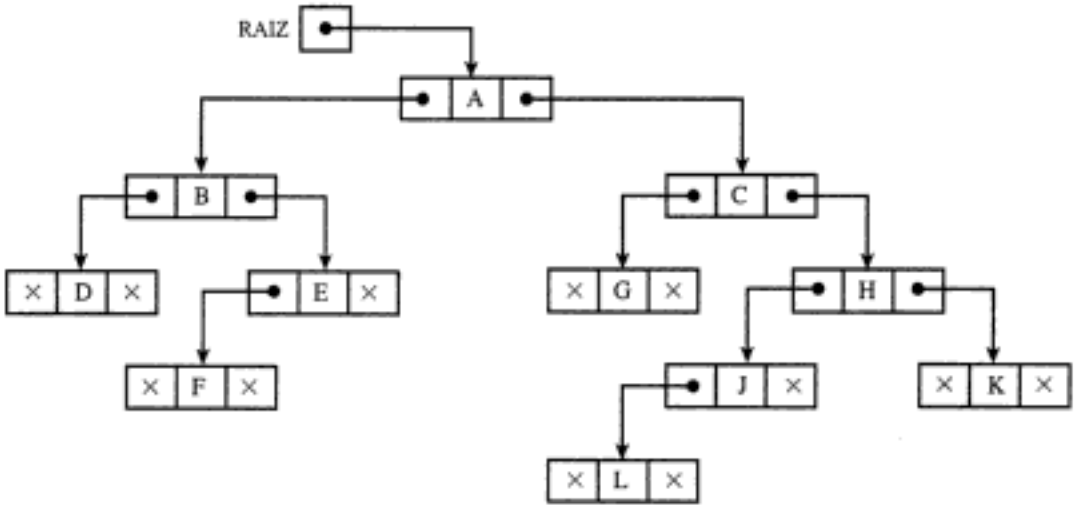


Fig. 10-6

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
INFO	*K*	*C*	*G*		*A*	*H*	*L*			*B*		*F*	*E*			*J*	*D*	
ESQ	0	3	0		10	16	0			17		0	12			7	0	
DIR	0	6	0		2	1	0			13		0	0			0	0	

RAIZ 5

Fig. 10-7

Representação Seqüencial de Árvores Binárias

Suponha que T é uma árvore binária completa ou quase completa. Então, existe uma maneira eficiente de manter T na memória denominada *representação seqüencial* de T. Essa representação utiliza apenas um único *array* linear ARVORE juntamente com um ponteiro variável FIM, como descrito a seguir.

(*a*) A raiz R de T é armazenada em ARVORE[1].

(*b*) Se um nó N ocupa ARVORE[K], então seu filho esquerdo é armazenado em ARVORE[$2 * K$], e seu filho direito é armazenado em ARVORE[$2 * K + 1$].

(*c*) FIM contém a posição do último nó de T.

Além disso, o nó N em ARVORE[K] contém uma subárvore esquerda ou direita vazia, dependendo de $2 * K$ ou $2 * K + 1$ ser maior do que FIM, ou ARVORE[$2 * K$] ou ARVORE[$2 * K + 1$] conter o valor NUL.

A representação seqüencial de uma árvore binária T, na Figura 10-8(*a*), aparece na Figura 10-8(*b*). Observe que necessitamos de 14 posições no *array* ARVORE apesar de T ter apenas nove nós. Em geral, a representação seqüencial de uma árvore de profundidade d usará um *array* com aproximadamente 2^d elementos. Conseqüentemente, esta representação normalmente é pouco eficiente, a menos que, como observado acima, a árvore binária seja completa ou quase completa. Por exemplo, a árvore T da Figura 10-1 tem 11 nós e profundidade 5, o que significa que será necessário um *array* com aproximadamente $2^5 = 32$ elementos.

Hidden page

Hidden page

10.6 ÁRVORES BINÁRIAS DE BUSCA

Esta seção discute uma das estruturas de dados mais importantes em ciência da computação, a árvore binária de busca. Essa estrutura permite procurar e localizar um elemento com um tempo de processamento de $f(n) = O(\log_2 n)$, onde n é o número de itens de dados. Também permite excluir e inserir elementos com facilidade. Essa estrutura contrasta com as seguintes estruturas:

(*a*) *Arrays lineares ordenados*: Aqui é possível procurar e localizar um elemento com tempo de processamento médio de $f(n) = O(\log_2 n)$. Entretanto, é custoso inserir e excluir elementos, já que, em média, isso envolve o movimento de $O(n)$ elementos.

(*b*) *Listas ligadas*: Aqui, pode-se facilmente inserir e excluir elementos. Entretanto, é custoso procurar e achar um elemento, uma vez que é necessário usar uma busca linear com tempo de processamento $f(n) = O(n)$.

Embora cada nó em uma árvore binária de busca possa conter um registro completo de dados, a definição da árvore depende de um campo dado cujos valores são distintos e podem estar ordenados.

Definição: Suponha que T é uma árvore binária. Então, T é dita uma árvore binária de busca se cada nó N de T tem a seguinte propriedade:

> O valor de N é maior do que qualquer valor na subárvore esquerda de N e é menor do que qualquer valor na subárvore direita de N.

Não é difícil entender que a propriedade acima garante que o percurso em em-ordem de T produzirá uma lista ordenada dos elementos de T.

Observação: A definição dada acima para uma árvore binária de busca assume que todos os valores dos nós são distintos. Existe uma definição análoga para uma árvore binária de busca T que admite duplicações, isto é, em que cada nó N tem as seguintes propriedades:

(*a*) $N > M$ para todo nó M em uma subárvore esquerda de N;
(*b*) $N \leq M$ para todo nó M em uma subárvore direita de N.

Quando esta definição é usada, as operações discutidas abaixo podem ser mudadas de forma compatível.

Exemplo10.5 A árvore binária T da Figura 10-11(*a*) é uma árvore binária de busca. Isto é, todo nó N em T excede qualquer número na sua subárvore esquerda e é menor do que qualquer número na sua subárvore direita. Suponha que 23 seja substituído por 35. Neste caso, T continuaria a ser uma árvore binária de busca. Por outro lado, suponha que 23 seja substituído por 40. Então, T deixaria de ser uma árvore binária de busca, já que 40 estaria na subárvore esquerda de 38, mas $40 > 38$.

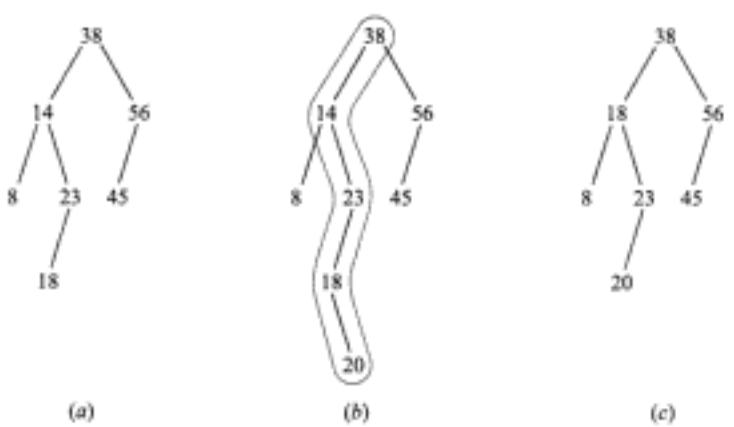


Fig. 10-11

(*a*) ***Localização e inserção em uma árvore binária de busca:*** O algoritmo a seguir é próprio para localização e inserção em uma árvore binária de busca.

Algoritmo 10.6A: São dados uma árvore binária de busca T e um ITEM de informação. O algoritmo acha a localização de ITEM em T ou insere ITEM como um novo nó.

Passo 1 Compare ITEM com a raiz N da árvore.

(*a*) Se ITEM < N, siga para o filho esquerdo de N.

(*b*) Se ITEM > N, siga para o filho direito de N.

Passo 2 Repita o Passo 1 até que uma das opções seguintes ocorra:

(*a*) Encontrou-se um nó N tal que ITEM = N. Neste caso, a busca foi bem-sucedida.

(*b*) Encontrou-se uma subárvore vazia, que indica que não ocorreu a localização. Insira ITEM no lugar da subárvore vazia.

Passo 3 Saia.

Exemplo 10.6 Considere a árvore binária de busca T da Figura 10-11(*a*). Suponha que seja dado ITEM = 20 e que queiramos localizar ou inserir ITEM em T. Simulando o Algoritmo 10.6A, obtemos os seguintes passos:

(1) Compare ITEM = 20 com a raiz R = 38. Como 20 < 38, siga para o filho esquerdo de 38, que é 14.
(2) Compare ITEM = 20 com 14. Como 20 > 14, siga para o filho direito de 14, que é 23.
(3) Compare ITEM = 20 com 23. Como 20 < 23, siga para o filho esquerdo de 23, que é 18.
(4) Compare ITEM = 20 com 18. Como 20 > 18, e 18 não tem filho direito, insira 20 como filho direito de 18.

A Figura 10-11(*b*) mostra a nova árvore com ITEM = 20 inserido. O caminho percorrido pelo algoritmo foi circundado.

(*a*) ***Exclusão em uma árvore binária de busca:*** O algoritmo a seguir deleta um ITEM dado de uma árvore binária de busca T; usa o algoritmo 10.6A para localizar ITEM em T.

Algoritmo 10.6B: São dados uma árvore binária T e um ITEM de informação. $P(N)$ denota o pai de um nó N, e $S(N)$ denota o sucessor em-ordem de N. O algoritmo deleta ITEM de T.

Passo 1 Use o Algoritmo 10.6A para localizar o nó N que contém ITEM e mantenha o percurso até a posição do nó pai $P(N)$. (Se ITEM não estiver em T, pare e saia.)

Passo 2 Determine o número de filhos de N. Existem três casos:

(*a*) N não tem filhos. N é deletado de T simplesmente substituindo a posição de N no nó pai $P(N)$ pelo ponteiro nulo.

(*b*) N tem exatamente um filho M. N é deletado de T substituindo a posição de N no nó pai $P(N)$ pela posição de M. (Isso substitui N por M.)

(*c*) N tem dois filhos.

(i) Ache o sucessor em-ordem $S(N)$ de N.
(Neste caso, $S(N)$ não tem filho esquerdo.)

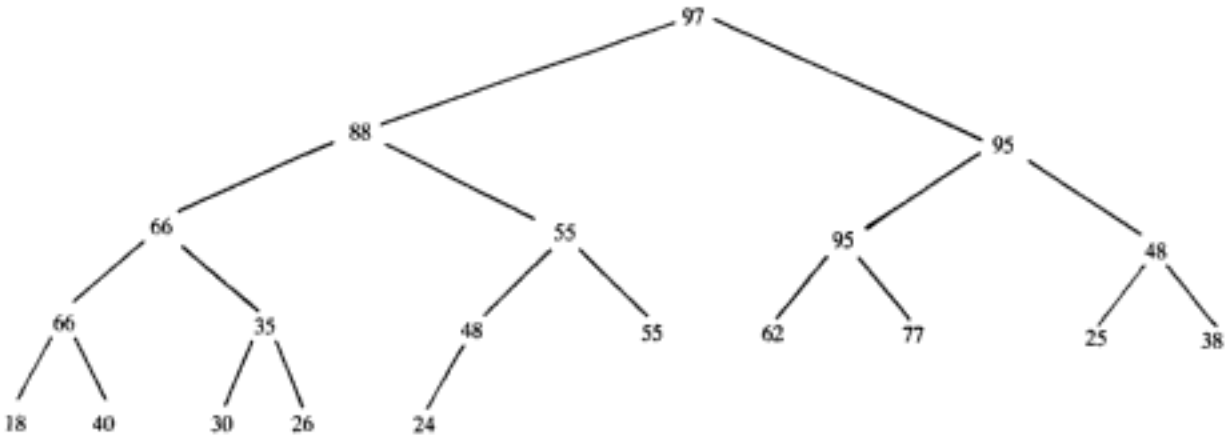
(ii) Delete $S(N)$ de T usando (*a*) ou (*b*).

(iii) Substitua N por $S(N)$ em T.

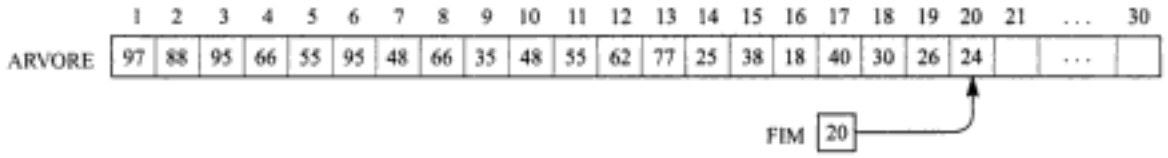
Passo 3 Saia.

Observação: Observe que o caso (iii) do passo 2(*c*) é mais complicado que os dois primeiros casos. O sucessor em-ordem $S(N)$ de N é achado como descrito a seguir. Partindo do nó N, mova-se à direita para o filho direito de N, e depois mova-se à esquerda, sucessivamente, até encontrar um nó M que não tenha filho esquerdo. O nó M é o sucessor em-ordem $S(N)$ de N.

Hidden page



(*a*) *Heap*



(*b*) Representação seqüencial

Fig. 10-12

(*a*) ARVORE[1] é a raiz R de H.

(*b*) ARVORE[2K] e ARVORE[2K + 1] são os filhos esquerdo e direito de ARVORE[K].

(*c*) A variável FIM = 20 indica o último elemento de H.

(*d*) O pai de qualquer nó, ARVORE[J], diferente da raiz, é o nó ARVORE[$J \div 2$] (onde $J \div 2$ significa divisão inteira).

Observe que os nós de H do mesmo nível aparecem, um após o outro, no *array* ARVORE. A escolha de 30 posições para ARVORE é arbitrária.

(*a*) ***Inserção em uma heap*:** O algoritmo seguinte insere um ITEM de informação dado em uma *heap* H.

Algoritmo 10.7A: São dados uma *heap* H e um novo ITEM. O algoritmo insere ITEM em H.

Passo 1 Junte ITEM ao final de H de tal modo que H continue a ser uma árvore completa, mas não necessariamente uma *heap*.

Passo 2 ("*Reheap*") Deixe ITEM "subir" até o seu "lugar apropriado" em H de tal modo que H seja uma *heap*.

(*a*) Compare ITEM com seu pai P(ITEM), se ITEM > P(ITEM), troque as posições de ITEM e P(ITEM).

(*b*) Repita (*a*) até que ITEM ≤ P(ITEM).

Passo 3 Saia.

Observação: É possível verificar que o algoritmo acima sempre produz uma *heap* ao final. Não é difícil perceber esse fato, e deixamos sua verificação ao leitor.

Exemplo 10.9 Considere a *heap* H da Figura 10-12. Suponha que queremos inserir ITEM = 70 em H. Simulando o Algoritmo 10.7A, primeiramente juntamos ITEM como último elemento da árvore completa; isto é, fazemos ARVORE[21] = 70 e FIM = 21. Então, voltamos a construir uma *heap*, isto é, fazemos ITEM "subir" até uma posição apropriada como a seguir:

(1) Compare ITEM = 70 com seu pai 48. Como 70 > 48, trocamos 70 com 48.
(2) Compare ITEM = 70 com seu novo pai 55. Como 70 > 55, trocamos 70 com 55.
(3) Compare ITEM = 70 com seu pai 88. Como 70 < 88, ITEM = 70 chegou ao local apropriado em H.

Hidden page

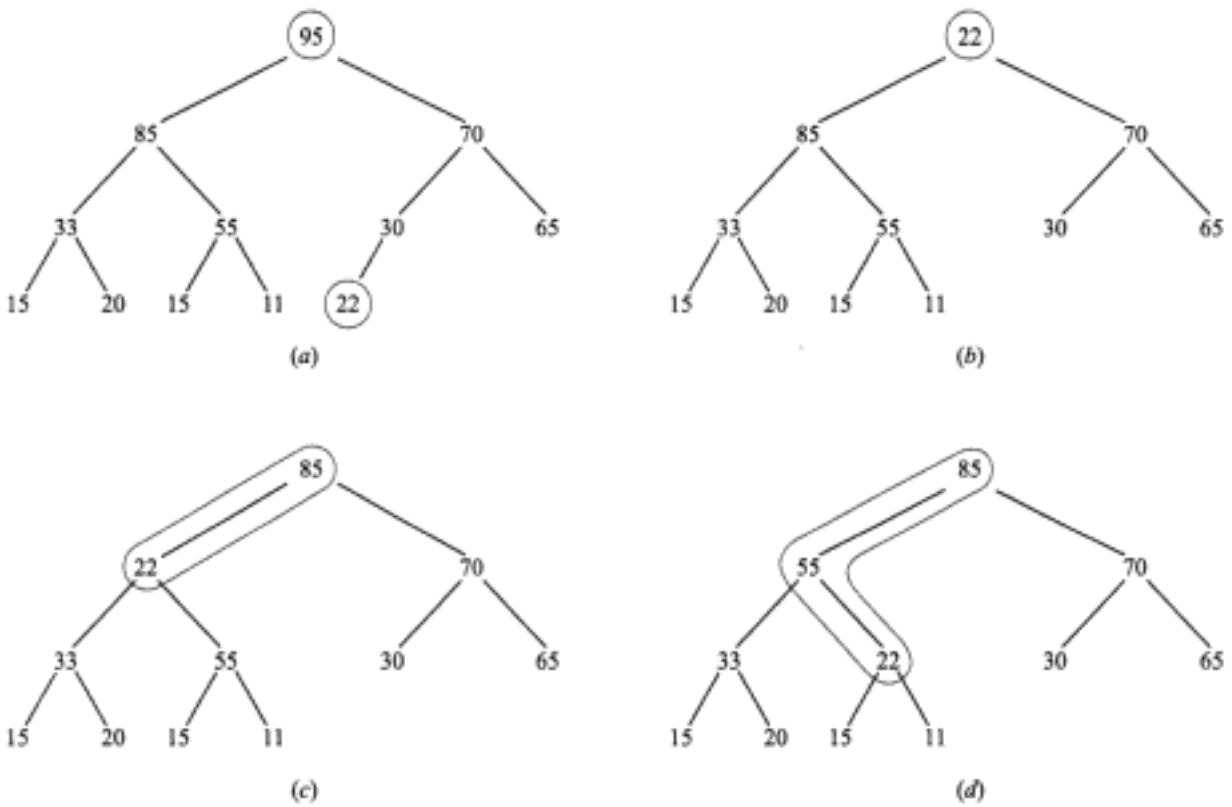


Fig. 10-14

Complexidade de Algoritmos para Heaps

Seja H uma *heap* com n nós. Como H é uma árvore completa, $d \approx \log_2 n$, onde d é a profundidade de H. O Algoritmo 10.7A nos diz para deixar ITEM percorrer "árvore acima", nível por nível, até achar seu lugar apropriado em H. O algoritmo 10.7B nos diz para deixar o último nó original, L, percorrer "árvore abaixo", nível por nível, até encontrar seu lugar apropriado em H. Em qualquer um dos casos o número de movimentos não pode exceder a profundidade d de H. Logo, o tempo de processamento $f(n)$ de qualquer um dos dois algoritmos é bem curto; especificamente, $f(n) = O(\log_2 n)$. Conseqüentemente, uma *heap* é uma maneira bem mais eficiente de implementar uma fila de prioridades S comparada tanto ao *array* linear quanto ao *array* linear ordenado, mencionados no início da seção.

10.8 COMPRIMENTO DE CAMINHOS E ALGORITMO DE HUFFMAN

Seja T uma árvore binária estendida ou uma 2-árvore (Seção 10-3). Isto é, T é uma árvore binária em que cada nó N tem zero ou dois filhos. Os nós sem filhos são denominados *nós externos*, e os nós com dois filhos são ditos *nós internos*. Às vezes, os nós são diferenciados nos diagramas pelo uso de círculos para nós internos e quadrados para nós externos. Além disso, se T tem n nós externos, então T tem $n - 1$ nós internos. A Figura 10-15 mostra uma 2-árvore com sete nós externos e, portanto, $7 - 1 = 6$ nós internos.

Hidden page

O algoritmo de Huffman, descrito a seguir, é definido recursivamente em termos do número n de pesos. Na prática, usamos uma forma iterativa, equivalente ao algoritmo de Huffman, que constrói a árvore desejada T da parte mais baixa para a mais alta, em vez de do alto para baixo.

Algoritmo 10.8: (Huffman) O algoritmo acha recursivamente uma 2-árvore T com n pesos dados $w_1, w_2, \ldots, w_n$ que tem um comprimento mínimo de caminho ponderado.

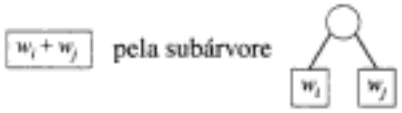
Passo 1 Suponha que $n = 1$. Faça T a árvore com um nó N com peso w_1, então Saia.

Passo 2 Suponha $n > 1$.

(*a*) Ache dois pesos mínimos, digamos w_i e w_j, entre os n pesos dados.

(*b*) Ache a árvore T' com o comprimento de caminho ponderado mínimo para os $n - 1$ pesos.

(*c*) Na árvore T', substitua o nó externo



(*d*) Saia.

Exemplo 10.12 Sejam A, B, C, D, E, F, G, H oito itens de dados com a seguinte atribuição de pesos:

Dados:	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*
Peso:	22	5	11	19	2	11	25	5

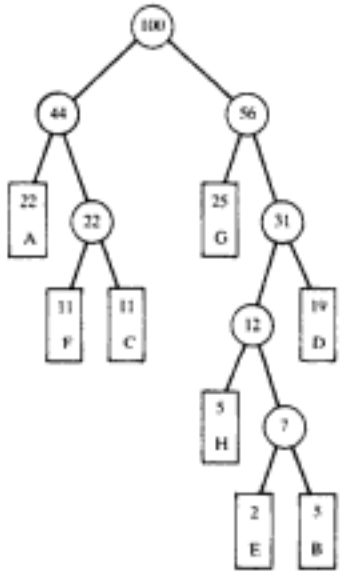
Construa uma 2-árvore T com comprimento de caminho ponderado mínimo P usando os dados acima como nós externos.

Aplique o algoritmo de Huffman. Isto é, combine repetidamente as duas subárvores de peso mínimo em uma única subárvore como mostrado na Figura 10-17(*a*). Por clareza, os pesos originais estão sublinhados, e um número circundado indica a raiz de uma nova subárvore. A árvore T é desenhada retrocedendo a partir do Passo 8 e produzindo a Figura 10-17(*b*). (Em caso de divisão de um nó em duas partes, desenhamos o menor nó à esquerda.) O comprimento do caminho P é:

$$P = 22(2) + 11(3) + 11(3) + 25(2) + 5(4) + 2(5) + 5(5) + 19(3) = 280$$

(1) 22, 5, 11, 19, 2, 11, 25, 5
(2) 22, 11, 19, (7), 11, 25, 5
(3) 22, 11, 19, 11, 25, (12)
(4) 22, 19, (22), 25, 12
(5) 22, (31), 22, 25
(6) 31, (44), 25
(7) 44, (56)
(8) (100)

(*a*) Algoritmo de Huffman



(*b*) Árvore T

Fig. 10-17

Hidden page

Exemplo 10.13 Considere de novo os oito itens de dados *A*, *B*, *C*, *D*, *E*, *F*, *G*, *H* do Exemplo 10.12. Suponha que os pesos representam as probabilidades percentuais de que um item ocorrerá. Usando *bits* para rotular as arestas da árvore de Huffman na Figura 10-17(*b*), obtemos a árvore *T* na Figura 10-19. O leitor pode verificar que a árvore *T* produz o seguinte código:

A: 00,	*B*: 11011,	*C*: 011,	*D*: 111
E: 11010,	*F*: 010,	*G*: 10,	*H*: 1100

Essa é uma codificação eficiente dos itens de dados.

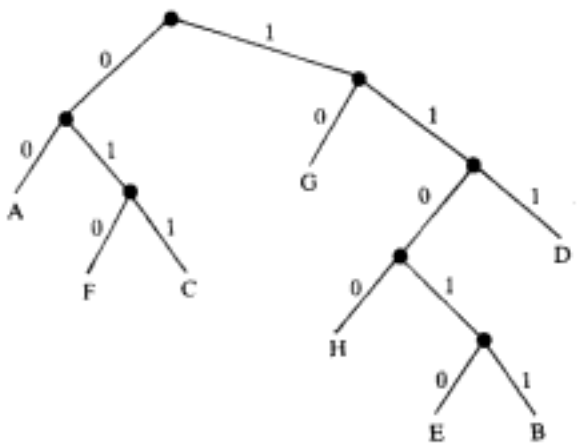


Fig. 10-19

10.9 ÁRVORES GERAIS (ORDENADAS COM RAÍZES) REVISITADAS

Seja *T* uma árvore ordenada com raízes (Seção 9-4), também conhecida como *árvore geral*[†]. *T* pode ser formalmente definida como um conjunto não vazio de elementos, chamados nós, tais que:

(1) Distingue-se em *T* um elemento *R*, chamado de raiz de *T*.
(2) Os outros elementos de *T* formam uma coleção ordenada de zero ou mais árvores disjuntas $T_1, T_2, \ldots, T_m$.

As árvores $T_1, T_2, \ldots, T_m$ são ditas *subárvores* da raiz *R*, e as raízes de $T_1, T_2, \ldots, T_m$ são denominadas *sucessores* de *R*.

A terminologia de relações de parentesco, de teoria de grafos e de horticultura é usada para árvores gerais da mesma forma que para árvores binárias. Em particular, se *N* é um nó com sucessores $S_1, S_2, \ldots, S_m$, então *N* é dito o *pai* de S_i, S_i é denominado *filho* de *N*, e os nós S_i são ditos *irmãos* um do outro.

Exemplo 10.14 A Figura 10-20 é uma representação gráfica de uma árvore geral *T* com 13 nós.

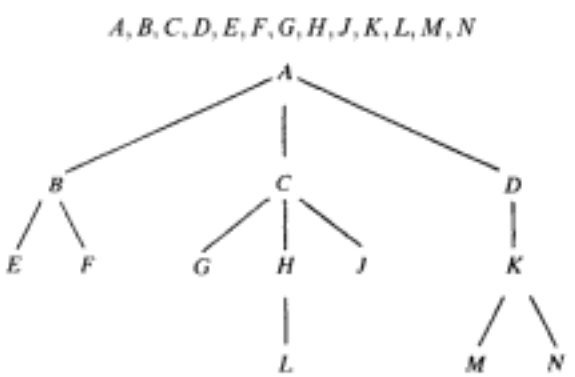


Fig. 10-20

[†] N. de T. No original, *general*; às vezes chamadas de genéricas.

A menos que haja especificação em contrário, a raiz da árvore T é o nó no topo do diagrama, e os filhos de um nó são ordenados da esquerda para a direita. Conseqüentemente, A é a raiz de T, e A tem três filhos: o primeiro filho B, o segundo filho C e o terceiro filho D. Observe que:

(*a*) O nó C tem três filhos.

(*b*) Cada um dos nós B e K tem dois filhos.

(*c*) Cada um dos nós D e H tem apenas um filho.

(*d*) Os nós E, F, G, L, J, M e N não têm filhos.

Os nós do último grupo, que não têm filhos, são chamados *nós terminais*.

Observação: Uma árvore binária T' não é um caso particular de uma árvore geral T. Elas são objetos distintos. As duas diferenças fundamentais são:

(1) Uma árvore binária T' pode ser vazia, mas uma árvore geral T é sempre não-vazia.

(2) Suponha que um nó N tenha apenas um filho. Então, em uma árvore binária T, este nó é distinguido como sendo o filho esquerdo ou direito; tal distinção não é feita em uma árvore geral.

A segunda diferença está ilustrada pelas árvores T_1 e T_2 na Figura 10-21. Especificamente, como árvores binárias, T_1 e T_2 são diferentes, uma vez que B é o filho esquerdo de A na árvore T_1, mas B é o filho direito de A na árvore T_2. Por outro lado, não existe diferença entre T_1 e T_2 como árvores gerais.

(*a*) Árvore T_1 (*b*) Árvore T_2

Fig. 10-21

Floresta

Uma *floresta*[†] F é definida como sendo uma coleção ordenada de zero ou mais árvores distintas. Evidentemente, se deletarmos a raiz R de uma árvore geral T, obtemos a floresta F que consiste nas subárvores de R (que podem ser vazias). Conversamente, se F é uma floresta, pode-se acrescentar um nó R a F para formar a árvore geral T, onde R é a raiz de T, e as subárvores de R consistem nas árvores originalmente em F.

Representação Computacional de Árvores Gerais

Suponha que T é uma árvore geral. A menos que especificação em contrário seja feita ou esteja implícita, T será mantida na memória por meio de uma representação ligada que usa três *arrays* paralelos INFO, FILHO e IRMAO e um ponteiro variável RAIZ, como a seguir. Primeiramente, cada nó N de T corresponderá a uma posição K tal que:

(1) INFO[K] contém o dado do nó N.

(2) FILHO[K] contém a posição do primeiro filho de N. A condição FILHO[K] = NUL indica que N não tem filhos.

(3) IRMAO[K] contém a posição do próximo irmão de N. A condição IRMAO[K] = NUL indica que N é o último filho de seu pai.

[†] N. de T. No original, *forest*. Usamos aqui a tradução literal; em muitos textos em português, define-se floresta como sendo um grafo sem circuitos, definindo-se então uma árvore como uma floresta conexa.

Hidden page

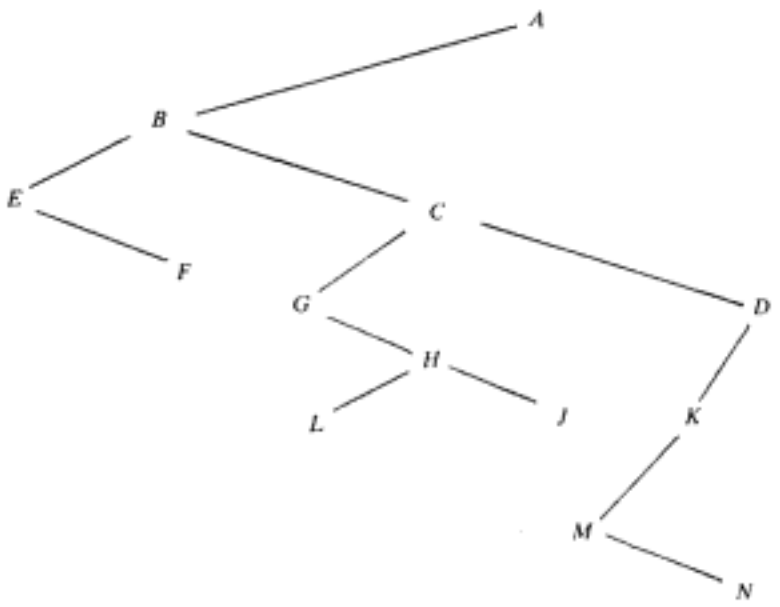


Fig. 10-23 Árvore binária T'.

Problemas Resolvidos

Árvores Binárias

10.1 Suponha que T seja uma árvore binária armazenada na memória como na Figura 10-24. Desenhe o diagrama de T.

A árvore T é desenhada a partir da raiz no sentido descendente como a seguir:

(*a*) A raiz R é obtida do valor do ponteiro RAIZ. Note que RAIZ = 5. Portanto, INFO[5] = 60 é a raiz R de T.

(*b*) O filho esquerdo de R é obtido do campo esquerdo de ponteiro de R. Note que ESQ[5] = 2. Portanto, INFO[2] = 30 é o filho esquerdo de R.

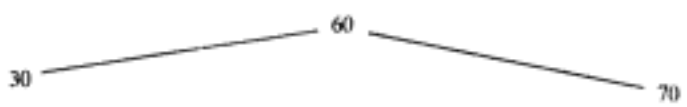
(*c*) O filho direito de R é obtido do campo direito de ponteiro de R. Note que DIR[5] = 6. Portanto, INFO[6] = 70 é o filho direito de R.

Podemos agora desenhar o topo da árvore como na Figura 10-25(*a*). Repetindo o processo acima com cada novo nó, obtemos finalmente a árvore solicitada T como na Figura 10-25(*b*).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
INFO	20	30	40	50	60	70	80	90			35	45	55	95
ESQ	0	1	0	0	2	0	0	7			0	3	11	0
DIR	0	13	0	0	6	8	0	14			12	4	0	0

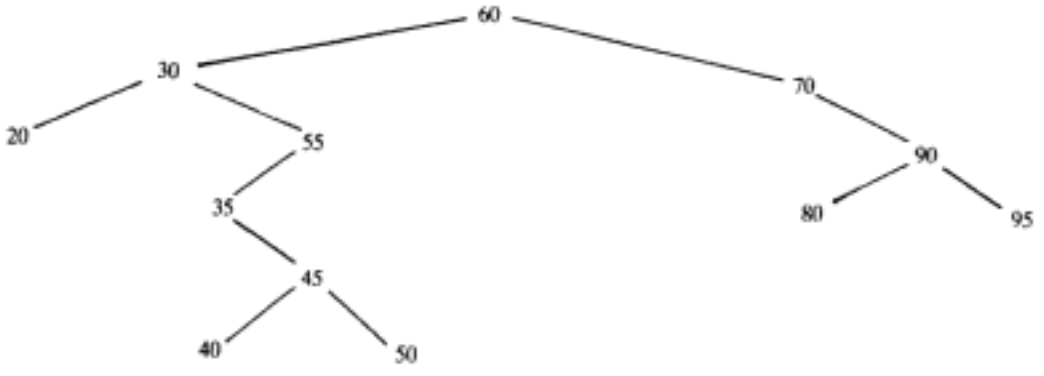
RAIZ 5

Fig. 10-24



(*a*)

Fig. 10-25 (1 de 2)



(*b*)

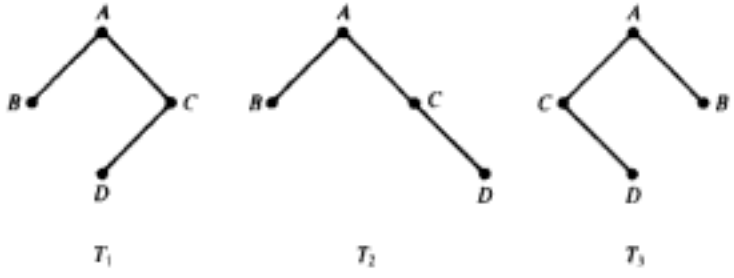
Fig. 10-25 (2 de 2)

10.2 Considere as árvores T_1, T_2, T_3 da Figura 10-26. Identifique as que representam a mesma: (*a*) árvore com raízes, (*b*) árvore ordenada com raízes, (*c*) árvore binária.

(*a*) Todas representam a mesma árvore com raízes, isto é, *A* é a raiz com filhos (sucessores imediatos) *B* e *C*, e *C* tem um único filho *D*.

(*b*) Aqui, T_1 e T_2 são a mesma árvore ordenada com raízes, mas T_3 é diferente. Especificamente, *B* é o primeiro filho de *A* em T_1, e T_2 é o segundo filho de *A* em T_3.

(*c*) Como árvores binárias, são todas diferentes. Especificamente, T_1 e T_2 são diferentes uma vez que distinguimos entre sucessores direito e esquerdo, mesmo quando existe apenas um sucessor (o que não é verdade para árvores ordenadas com raízes). Isto é, *D* é o sucessor esquerdo de *C* em T_1, mas é sucessor direito de *C* em T_2.



T_1 T_2 T_3

Fig. 10-26

10.3 Considere a árvore binária *T* da Figura 10-27. Ache a representação seqüencial de *T* na memória.

A representação seqüencial de *T* usa apenas um único *array* linear ARVORE junto com um ponteiro variável FIM.

(*a*) A raiz *R* de *T* está armazenada em ARVORE[1]; portanto, ARVORE[1] = *F*.

(*b*) Se o nó *N* ocupa ARVORE[*K*], seus filhos esquerdo e direito estão armazenados em ARVORE[$2 * K$] e ARVORE[$2 * K + 1$], respectivamente. Logo, ARVORE[2] = *A* e ARVORE[3] = *D*, já que *A* e *D* são os filhos esquerdo e direito de *F*, e assim por diante. A Figura 10-28 contém a representação seqüencial de *T*. Note que ARVORE[10] = *C*, pois *C* é o filho esquerdo de *K* que está armazenado em ARVORE[5]. Além disso, ARVORE[4] = *B* e ARVORE[15] = *E*, pois *B* e *E* são os filhos esquerdo e direito de *G*, que está armazenado em ARVORE[7].

(*c*) FIM aponta para a localização do último nó de *T*; logo, FIM = 15.

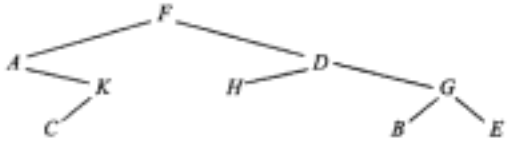
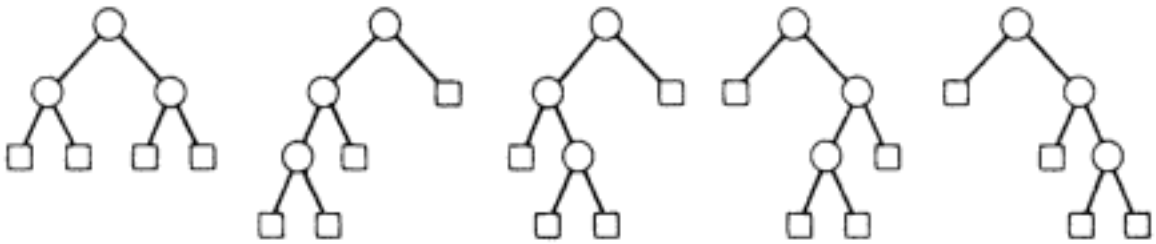


Fig. 10-27

Hidden page

Hidden page



(*b*) Árvores binárias estendidas com quatro nós externos

Fig. 10-31 (2 de 2)

Árvores Binárias de Busca, Heaps

10.8 Considere a árvore binária T da Figura 10-25(*b*).

(*a*) Por que T é uma árvore binária de busca?

(*b*) Suponha que ITEM = 33 seja inserido na árvore. Ache a nova árvore T.

(*a*) T é uma árvore binária de busca porque cada nó N é maior do que os valores na sua subárvore esquerda e menor do que os valores na sua subárvore direita.

(*b*) Compare ITEM = 33 com a raiz 60. Como 33 < 60, vá para o filho esquerdo 30. Como 33 < 60, vá para o filho direito, 55. Como 33 < 55, vá para o filho esquerdo, 35, que, entretanto, não tem filho esquerdo. Portanto, coloque ITEM = 33 como filho esquerdo do nó 35 para obter a árvore da Figura 10-32. As arestas sombreadas indicam o caminho, árvore abaixo, durante a inserção.

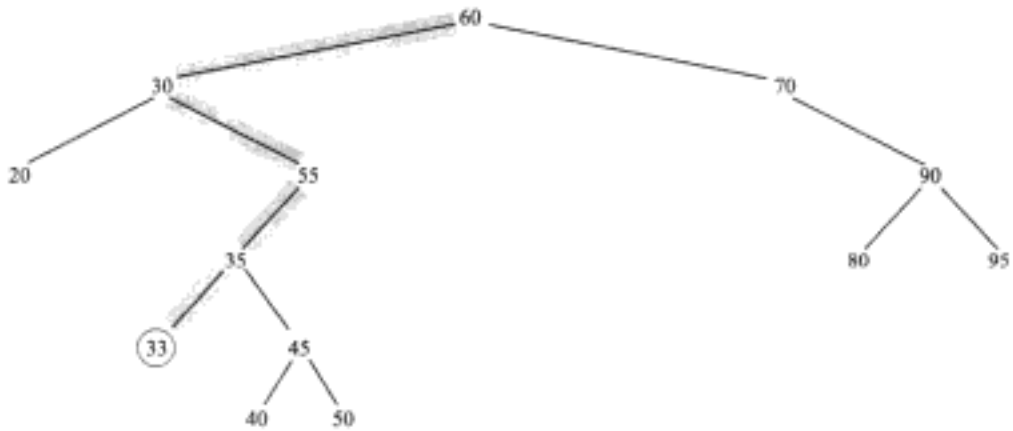


Fig. 10-32

10.9 Suponha que a seguinte lista de letras é inserida em uma árvore binária de busca vazia:

$$J, \quad R, \quad D, \quad G, \quad W, \quad E, \quad M, \quad H, \quad P, \quad A, \quad F, \quad Q$$

(*a*) Ache a árvore final T. (*b*) Determine o percurso em em-ordem de T.

(*a*) Insira os nós, um após o outro, para obter a árvore da Figura 10-33.

(*b*) O percurso em em-ordem de T é:

$$A, \quad D, \quad E, \quad F, \quad G, \quad H, \quad J, \quad M, \quad P, \quad Q, \quad R, \quad W$$

Observe que essa é uma lista alfabética de letras. (O percurso em em-ordem de qualquer árvore binária de busca T produz uma lista ordenada de nós.)

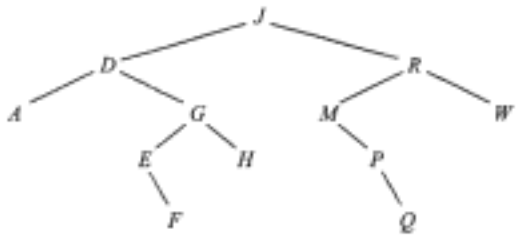


Fig. 10-33

10.10 Considere a árvore binária de busca T da Figura 10-33. Descreva a árvore T depois de: (*a*) o nó M ser deletado; (*b*) o nó D ser deletado.

(*a*) O nó M tem apenas um filho, P. Portanto, delete M e deixe P como filho esquerdo de R no lugar de M.

(*b*) O nó D tem dois filhos. Ache o sucessor em-ordem de D, que é o nó E. Primeiramente delete E da árvore, e depois substitua-o por D.

A Figura 10-34 mostra a árvore atualizada T.

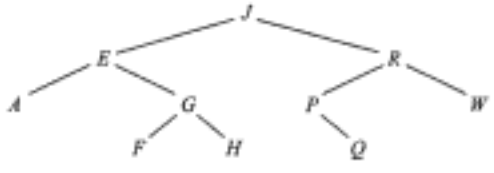


Fig. 10-34

Fig. 10-35

10.11 Suponha que n itens de dados $A_1, A_2, \ldots, A_N$ estão ordenados, i.e., $A_1 < A_2 < \cdots < A_N$.

(*a*) Se os itens são inseridos em uma árvore binária vazia T, descreva a árvore final T.

(*b*) Qual é a profundidade d da árvore final T?

(*c*) Compare d com a profundidade média d^* de uma árvore binária com n nós para (i) $n = 50$; (ii) $n = 100$; (iii) $n = 500$.

(*a*) A árvore T consiste em um ramo que se estende para a direita, como desenhado na Figura 10-35.

(*b*) O ramo de T tem n nós; logo, $d = n$.

(*c*) É sabido que $d^* = c \log_2 n$, onde $c \approx 1{,}4$. Logo:

(i) $d(50) = 50$; $d^*(50) \approx 9$.

(ii) $d(100) = 100$; $d^*(100) \approx 10$.

(iii) $d(500) = 500$; $d^*(500) \approx 12$.

10.12. Considere a *minheap* H da Figura 10-36(*a*). (H é uma *minheap* já que no topo estão os menores elementos, e não os maiores.) Descreva a *heap* depois que ITEM 11 é inserido em H.

Primeiramente insira ITEM como filho esquerdo do nó 44. Então, compare, repetidamente, ITEM com seu PAI, e troque ITEM e PAI enquanto ITEM < PAI. Como 11 < 44, troque 11 e 44. Como 11 < 22, troque 11 e 22. Como 11 > 8, ITEM = 11 chegou ao seu lugar na *heap* H. A Figura 10-36(*b*) mostra a *heap* final H. As arestas sombreadas indicam o caminho de ITEM na árvore.

Hidden page

Comprimento de Caminhos, Algoritmo de Huffman

10.14 Considere a 2-árvore ponderada T da Figura 10-39. Ache o comprimento do caminho ponderado P da árvore T.

Multiplique cada peso W_i pelo comprimento L_i do caminho da raiz T ao nó contendo o peso, depois some todos os produtos para obter P. Logo,

$$P = 4(2) + 15(4) + 25(4) + 5(3) + 8(2) + 16(2)$$
$$= 8 + 60 + 100 + 15 + 16 + 32 = 231$$

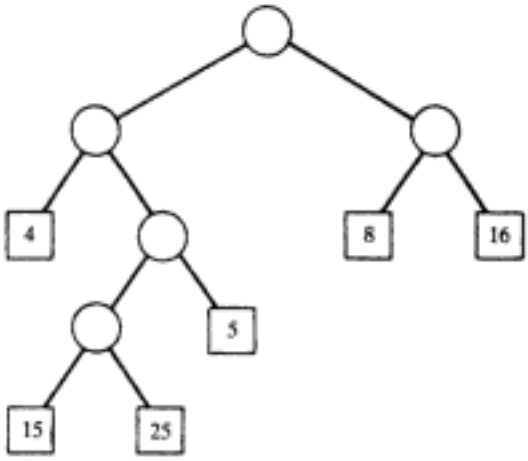


Fig. 10-39

10.15 Suponha que são dados seis pesos: 4, 15, 25, 5, 8 e 16. Ache uma 2-árvore com os pesos dados e um comprimento de caminho mínimo P. (Compare T com a árvore na Figura 10-39.)

Use o algoritmo de Huffman. Isto é, combine repetidamente as duas subárvores com pesos mínimos em uma única subárvore como a seguir:

(*a*) 4, 15, 25, 5, 8, 16

(*b*) 15, 25, (9), 8, 16

(*c*) 15, 25, (17), 16

(*d*) 25, 17, (31)

(*e*) (42), 31

(*f*) (73)

(Os números circundados indicam a raiz da nova subárvore no passo.) A árvore T está desenhada do Passo (*f*) para trás, produzindo a Figura 10-40. Com a árvore T, compute:

$$P = 25(2) + 4(4) + 5(4) + 8(3) + 15(2) + 16(2)$$
$$= 50 + 16 + 20 + 24 + 30 + 32 = 172$$

(A árvore da Figura 10-39 tem comprimento de caminho 231.)

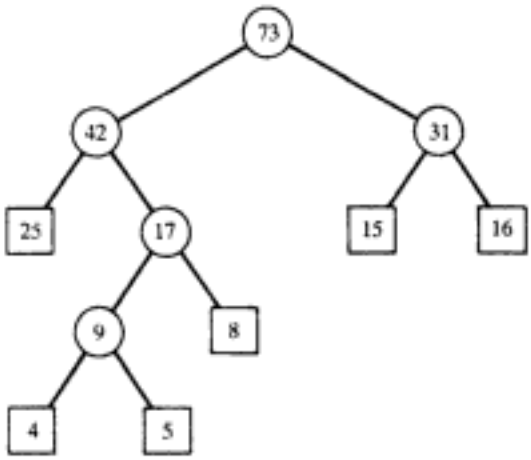


Fig. 10-40

10.16 Suponha que os itens de dados A, B, C, D, E, F e G ocorrem com a seguinte distribuição de probabilidades:

Item de dados:	A	B	C	D	E	F	G
Probabilidade:	10	30	5	15	20	15	5

Ache um código de Huffman para os dados.

Aplique o algoritmo de Huffman para achar uma 2-árvore T com o mínimo comprimento de caminho ponderado P como a seguir.

(*a*) 10, 30, 5, 15, 20, 15, 5

(*b*) 10, 30, (10), 15, 20, 15

(*c*) (20), 30, 15, 20, 15

(*d*) 20, 30, (30), 20

(*e*) (40), 30, 30

(*f*) 40 (60)

(*g*) (100)

(Novamente, os números circundados indicam a raiz da nova subárvore no passo.) A árvore T está desenhada a partir do Passo (*g*) para trás, produzindo a Figura 10-41. Atribua rótulos de *bits* aos ramos da árvore T, 0 ao ramo esquerdo, e 1 ao ramo direito, como na Figura 10-41. A árvore T produz o seguinte código de Huffman:

A: 000 B: 11 C: 0010 D: 100 E: 01 F: 101 G: 0011

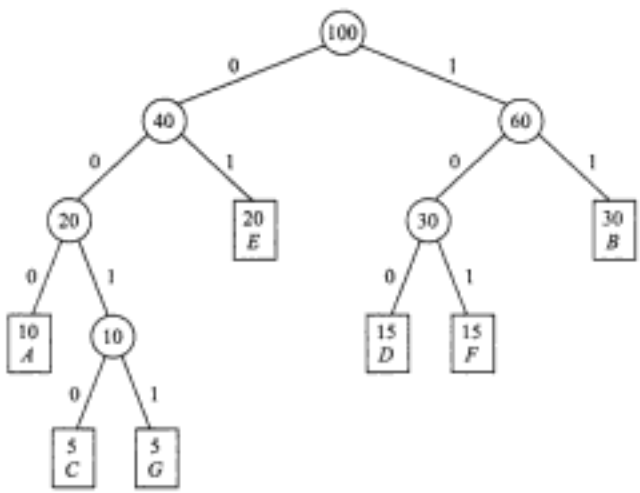


Fig. 10-41

Hidden page

Hidden page

10.24 Suponha que os percursos em pré-ordem e em-ordem de T produzem as seguintes seqüências de nós:

Pré-ordem: $G,\ B,\ Q,\ A,\ C,\ K,\ F,\ P,\ D,\ E,\ R,\ H$

Em-ordem: $Q,\ B,\ K,\ C,\ F,\ A,\ G,\ P,\ E,\ D,\ H,\ R$

(*a*) Desenhe o diagrama de T.

(*b*) Ache: (i) a profundidade de T; (ii) os descendentes de B.

(*c*) Liste os nós terminais de T.

10.25 Liste a 2-árvore T que corresponde à expressão algébrica $E = (x + 3y)^4(a - 2b)$, e ache a pré-ordem de T.

Árvores Binárias de Busca, Heaps

10.26 Ache a árvore final T se os seguintes nós são inseridos em uma árvore binária de busca T vazia.

50, 33, 44, 22, 77, 35, 60, 40

10.27 Considere a árvore binária de busca T da Figura 10-45. Suponha que os nós 20, 55 e 88 são inseridos, um após o outro, em T. Ache a árvore final T.

10.28 Considere a árvore binária de busca T da Figura 10-45. Suponha que os nós 22, 25 e 75 são deletados, um após o outro, de T. Ache a árvore final T.

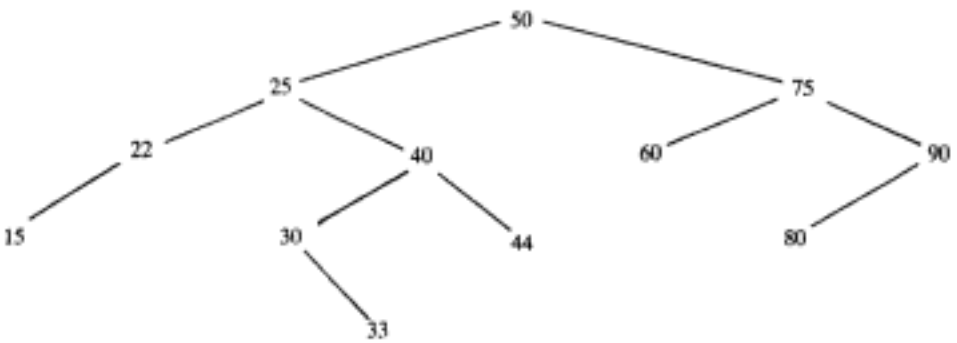


Fig. 10-45

10.29 Considere a árvore completa T com $N = 10$ nós da Figura 10-46.

(*a*) Ache a representação seqüencial de T no *array* A na memória.

(*b*) Forme, a partir de T, uma *maxheap* H pela inserção repetida de $A[J + 1]$ na *heap* $A[1]$ até $A[J]$ (como foi feito no Problema 10.13).

(*c*) Forme uma *minheap* H' (em vez de uma *maxheap*) a partir de T.

Fig. 10-46

Algoritmo de Huffman, Árvores Gerais

10.30 Considere a 2-árvore T da Figura 10-47 que contém as sete letras A, B, C, D, E, F, G como nós externos. Ache o código de Huffman das letras determinado pela árvore T.

10.31 Suponha que são atribuídos aos sete itens de dados, $A, B, \ldots, G$, os seguintes pesos:

$$(A, 13), \quad (B, 2), \quad (C, 19), \quad (D, 23), \quad (E, 29), \quad (F, 5), \quad (G, 9)$$

Ache o comprimento ponderado de caminho P na Figura 10-47.

10.32 Usando os dados do Problema 10-31, ache o código de Huffman para as sete letras usando a 2-árvore com o comprimento mínimo de caminho ponderado P e ache P.

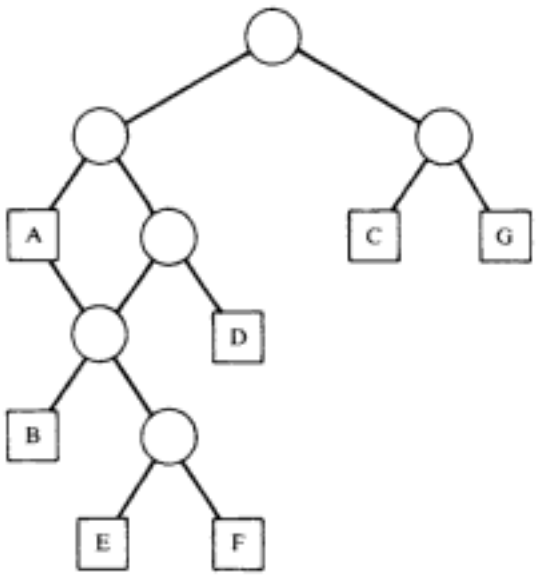


Fig. 10-47

10.33 Considere a floresta F, na Figura 10-48, que consiste em três árvores com raízes A, B e C, respectivamente. Desenhe a árvore binária F' correspondente a F.

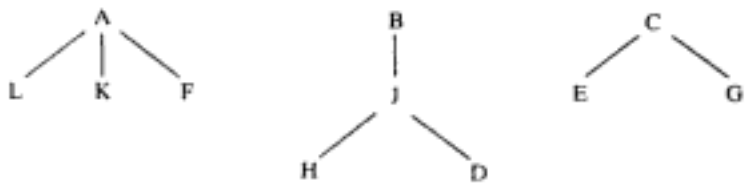


Fig. 10-48

Problemas Relativos a Computadores

Os Problemas 10-34 a 10-39 se referem à Figura 10-49, que é uma lista de registros de empregados armazenada na memória. A tabela representa uma árvore binária de busca no que se refere à chave NOME. Também usa um nó indicador que lista o número dos empregados em INSS[IND] e o salário total em SAL[IND]. Além disso, a fim de permitir inserções, as posições disponíveis (vazias) formam uma lista ligada onde VAZ aponta para o primeiro elemento da lista, e a seqüência é mantida pelo *array* ESQ.

Hidden page

Hidden page

Hidden page

Capítulo 11

Propriedades dos Inteiros

11.1 INTRODUÇÃO

Este capítulo investiga algumas propriedades básicas dos *números naturais* (ou *inteiros positivos*), isto é, o con
junto

$$\mathbf{N} = \{1, 2, 3, \ldots\}$$

e seus "primos", os inteiros, isto é, o conjunto

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

(A letra **Z** vem da palavra *Zahlen*, que significa "números" em alemão.)

Vamos assumir como conhecidas as seguintes regras simples sobre adição e multiplicação destes números:

(*a*) Lei Associativa para multiplicação e adição:

$$(a + b) + c = a + (b + c) \qquad \text{e} \qquad (ab)c = a(bc)$$

(*b*) Lei Comutativa para multiplicação e adição:

$$a + b = b + a \qquad \text{e} \qquad ab = ba$$

(*c*) Lei Distributiva:

$$a(b + c) = ab + ac$$

(*d*) Existência da identidade para adição e multiplicação:

$$a + 0 = 0 + a = a \qquad \text{e} \qquad a \cdot 1 = 1 \cdot a = a$$

(*e*) Existência do inverso em relação à adição, $-a$, para todo inteiro a:

$$a + (-a) = (-a) + a = 0$$

O próximo capítulo mostra que outras estruturas matemáticas têm as propriedades citadas. Uma propriedade fundamental que distingue os inteiros **Z** de outras estruturas é o princípio da indução matemática (Seção 1.10) que rediscutimos aqui. Também enunciamos e provamos (Problema 11.34) o teorema seguinte.

Teorema Fundamental da Aritmética: Todo inteiro positivo $n > 1$ pode ser escrito de maneira única como um produto de números primos.

Este teorema já aparecia em *Elementos*, de Euclides. Desenvolvemos também os conceitos e métodos que são usados para provar esse importante teorema.

11.2 ORDEM E DESIGUALDADES, VALOR ABSOLUTO

Esta seção discute as propriedades elementares de ordenação e valor absoluto.

Ordem

Sejam a e b inteiros. Dizemos que a é *menor* do que b e denota-se

$$a < b$$

se a diferença $b - a$ é positiva, isto é, $b - a$ pertence a **N**.

Observe que definimos ordem em **Z** em termos dos inteiros positivos **N**. Todas as propriedades usuais desta relação de ordem são conseqüência das duas seguintes propriedades de **N**:

[$\mathbf{P}_1$] Se a e b pertencem a **N**, então $a + b$ e ab pertencem a **N**.

[$\mathbf{P}_2$] Para todo inteiro a, ou $a \in \mathbf{N}$, ou $a = 0$ ou $-a \in \mathbf{N}$.

A seguinte notação também é usada:

$a > b$ significa $b < a$; lê-se a maior do que b.
$a \leq b$ significa $a < b$ ou $a = b$; lê-se a é menor ou igual a b.
$a \geq b$ significa $b \leq a$; lê-se a é maior ou igual a b.

As relações $<$, $>$, $\leq$ e $\geq$ são chamadas *desigualdades* para que sejam diferenciadas da relação $=$ de igualdade.

O leitor certamente está familiarizado com a representação dos inteiros como pontos em uma reta, chamada *reta numérica* **R**, como segue:

Notamos que $a < b$ se e somente se a está à esquerda de b na reta numérica acima. Por exemplo,

$$2 < 5; \quad -6 < -3; \quad 4 \leq 4; \quad 5 > -8; \quad 6 \geq 0; \quad -7 \leq 0$$

Também notamos que a é positivo sse $a > 0$, e a é negativo sse $a < 0$. (Lembre que "sse" significa "se e somente se".)

Propriedades básicas das relações de desigualdade são descritas a seguir.

Proposição 11.1: A relação $\leq$ em **Z** tem as seguintes propriedades:
(i) $a \leq a$ para qualquer inteiro a.
(ii) Se $a \leq b$ e $b \leq a$, então $a = b$.
(iii) Se $a \leq b$ e $b \leq c$, então $a \leq c$.

Proposição 11.2: (**Lei da Tricotomia**) Para quaisquer inteiros a e b, vale exatamente uma das seguintes afirmações:

$$a < b, \qquad a = b \qquad \text{ou} \qquad a > b$$

Proposição 11.3: Suponha que $a \leq b$, e seja c um inteiro qualquer. Então:
(i) $a + c \leq b + c$.
(ii) $ac \leq bc$ se $c > 0$, mas $ac \geq bc$, se $c < 0$.

(O Problema 11.6 demonstra a Proposição 11.3.)

Hidden page

$$P(1): \quad 1 = 1^2$$

Suponha que $P(n)$ é verdade. (Esta hipótese é conhecida como hipótese de indução.) Adicionando $2n + 1$ a ambos os lados de $P(n)$, obtemos

$$1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + (2n + 1)$$
$$= (n + 1)^2$$

que é $P(n + 1)$. Mostramos que $P(n + 1)$ é verdade sempre que $P(n)$ é verdade. Pelo princípio de indução matemática, P é verdade para todo n.

(*b*) O símbolo $n!$ (lê-se n fatorial) é definido como o produto dos primeiros n inteiros positivos, isto é:

$$1! = 1, \qquad 2! = 1 \cdot 2 = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad \text{e assim por diante}$$

Isto pode ser formalmente definido como a seguir:

$$1! = 1 \quad \text{e} \quad (n + 1)! = (n + 1)(n!) \text{ para } n > 1$$

Observe que, se S é o conjunto dos inteiros positivos para os quais ! é definido, então S satisfaz às duas propriedades de indução matemática. Logo, a definição acima define ! para todo inteiro positivo.

Existe uma outra forma do princípio de indução matemática (demonstrada no Problema 11.15) cujo uso, às vezes, é mais conveniente. A saber:

Teorema 11-5: **(Indução: segunda forma)** seja P uma proposição definida nos inteiros $n \geq 1$ tal que:
(i) $P(1)$ é verdade.
(ii) $P(n)$ é verdade sempre que $P(k)]$ é verdade para todo $1 \leq k < n$.
Então P é verdade para todo inteiro $n \geq 1$.

Observação: O teorema acima é verdade se o inteiro 1 é trocado por 0 ou por qualquer outro inteiro m.

Princípio da Boa Ordenação

Uma propriedade dos inteiros positivos que é equivalente ao princípio de indução, embora aparentemente muito diferente, é o princípio da boa ordenação (provado no Problema 11.14). A saber:

Teorema 11-6: **(Princípio da boa ordenação)** seja S um conjunto não vazio de inteiros positivos. Então S contém um *menor elemento*; isto é, S contém um elemento a tal que $a \leq s$ para todo s em S.

Em linhas gerais, um conjunto S é dito *bem ordenado* se todo subconjunto de S contém um primeiro elemento. Logo, o Teorema 11.6 afirma que **N** é bem ordenado.

Um conjunto S de inteiros é dito *inferiormente limitado* se todo elemento de S é maior do que algum inteiro m (que pode ser negativo). (O número m é dito o *limite inferior* de S.) Um corolário simples do teorema acima é o seguinte:

Corolário 11-7: seja S um conjunto não vazio de inteiros inferiormente limitado. Então S contém um menor elemento.

11.4 ALGORITMO DE DIVISÃO

A seguinte propriedade fundamental da aritmética (demonstrada nos Problemas 11.20 e 11.21) é, essencialmente, uma reafirmação do resultado do algoritmo de divisão longa[†].

Teorema 11-7: **(Algoritmo de divisão)** sejam a e b inteiros com $b \neq 0$. Existem inteiros q e r tais que:

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < |b|$$

[†] N. de T. No original, *long division*. Refere-se ao algoritmo de Euclides.

Além disso, os inteiros q e r são únicos.

O número q no teorema anterior é dito o *quociente*, e r é conhecido como *resto*. Reforçamos o fato de que r deve ser não negativo. O teorema também diz que:

$$a - bq = r$$

Essa equação será usada na próxima parte.

Se a e b são positivos, q é não negativo. Se q é positivo, então a Figura 11-1 dá uma interpretação geométrica desse teorema. Isto é, os múltiplos positivos e negativos serão distribuídos ao longo da linha **R**, e a estará entre dois múltiplos da forma qb e $(q + 1)b$. A distância entre qb e a é o resto r.

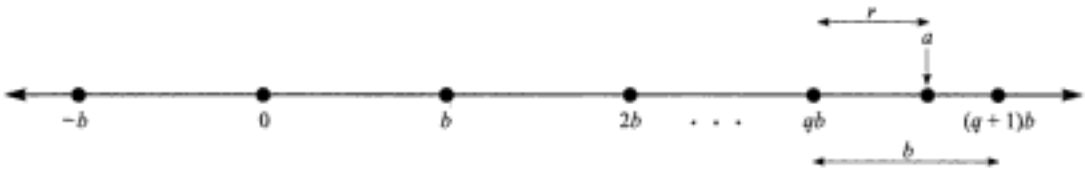


Fig. 11-1

Exemplo 11.2

(*a*) Seja $a = 4461$ e $b = 16$. Achamos $q = 278$ e $r = 13$, pelo algoritmo de divisão longa, digamos, como na Figura 11-2(*a*). Como esperado,

$$4461 = 16(278) + 13$$

Isto é, $a = bq + r$.

(*b*) Seja $a = -262$ e $b = 3$. Primeiramente dividimos 262 por 3 como na Figura 11-2(*b*). Essa divisão tem quociente 87 e resto 1. Portanto,

$$262 = 3(87) + 1$$

Precisamos de $a = -262$, e então multiplicamos por -1 obtendo

$$-262 = 3(-87) - 1$$

Entretanto, -1 é negativo e não pode ser r. Corrigimos esse problema adicionando e subtraindo o valor de b (que é 3) como a seguir:

$$-262 = 3(-87) - 3 + 3 - 1 = 3(-88) + 2$$

Portanto, $q = -88$ e $r = 2$.

(*c*) Seja $b = 2$. Então, todo inteiro a pode ser escrito da forma

$$a = 2q + r \qquad \text{e} \qquad 0 \leq r < 2$$

Logo, r só pode ser 0 ou 1. Logo, todo inteiro é da forma $2k$ ou $2k + 1$. Os inteiros da forma $2k$ são chamados de inteiros *pares*, enquanto os da forma $2k + 1$ são chamados de inteiros *ímpares*. (Normalmente, um inteiro par é definido como um inteiro divisível por 2, e todos os outros inteiros são ditos ímpares. O algoritmo de divisão mostra que todo inteiro ímpar tem a forma $2k + 1$.)

$$\begin{array}{r|l} 4461 & 16 \\ -32 & 278 \\ \hline 126 & \\ -112 & \\ \hline 141 & \\ -128 & \\ \hline 13 & \end{array} \qquad \begin{array}{r|l} 262 & 3 \\ -24 & 87 \\ \hline 22 & \\ -21 & \\ \hline 1 & \end{array}$$

(*a*) (*b*)

Fig. 11-2

Hidden page

Demonstração: A demonstração é feita por indução. Seja $n = 2$. Como 2 é primo, n é um produto de primos. Suponha que $n > 2$ e que o teorema vale para todos os inteiros positivos menores do que n. Se n é primo, então n é um produto de primos. Se n não é primo, então $n = ab$, onde $a, b < n$. Por indução, a e b são produtos de primos; portanto, $n = ab$ também é um produto de primos.

Euclides, que provou o Teorema Fundamental da Aritmética, também questionou a existência de um número primo máximo. Ele respondeu à pergunta da seguinte maneira:

Teorema 11-11: não existe um número primo máximo; isto é, existe um número infinito de primos.

Demonstração: Suponha que existe um número finito de primos, $p_1, p_2, \ldots, p_m$. Considere o inteiro

$$n = p_1 p_2 \cdots p_m + 1$$

Como n é um produto de primos (Teorema 11.10), ele é divisível por um dos primos, digamos, p_k. Note que p_k também divide o produto $p_1 p_2 \cdots p_m$. Portanto, p_k divide,

$$n - p_1 p_2 \cdots p_m = 1$$

Isso é impossível, e, logo, n é divisível por algum outro primo. Isso contradiz a hipótese de que $p_1, p_2, \ldots, p_m$ são os únicos primos. Portanto, o número de primos é infinito, e o teorema fica provado.

11.6 MÁXIMO DIVISOR COMUM E ALGORITMO DE EUCLIDES

Suponha que a e b são inteiros e que pelo menos um deles não é zero. Um inteiro d é dito um *divisor comum* de a e b se d divide ambos, isto é, $d|a$ e $d|b$. Note que 1 é um divisor comum positivo de a e b, e que qualquer divisor comum de a e b não pode ser maior do que $|a|$ ou $|b|$. Logo, existe um máximo divisor comum de a e b; ele é representado por

$$\text{mdc}(a, b)$$

e é dito o *máximo divisor comum* de a e b.

Exemplo 1.5

(*a*) Os divisores comuns de 12 e 18 são $\pm 1, \pm 2, \pm 3, \pm 6$. Logo

$$\text{mdc}\,(12, 18) = 6$$

Analogamente,

$$\text{mdc}\,(12, -18) = 6, \qquad \text{mdc}\,(12, -16) = 4, \qquad \text{mdc}\,(29, 15) = 1, \qquad \text{mdc}\,(14, 49) = 7$$

(*b*) Para todo inteiro a, temos $\text{mdc}(1, a) = 1$.

(*c*) Para todo primo p, temos

$$\text{mdc}\,(p, a) = p \qquad \text{ou} \qquad \text{mdc}\,(p, a) = 1$$

De acordo com o fato de $p|a$ ou $p \nmid a$.

(*d*) Suponha que a é positivo. Então, $a|b$ sse $\text{mdc}(a, b) = a$.
O teorema seguinte (provado no Problema 11.30) dá uma caracterização alternativa do máximo divisor comum.

Teorema 11-12: seja d o menor inteiro positivo da forma $ax + by$. Então, $d = \text{mdc}(a, b)$.

Corolário 11-13: suponha que $d = \text{mdc}(a, b)$. Então, existem inteiros x e y tais que $d = ax + by$.

Outra maneira de caracterizar o máximo divisor comum sem usar relação de desigualdade é a seguinte:

Teorema 11-14: um inteiro positivo $d = \text{mdc}(a, b)$ se e somente se tem as duas propriedades seguintes:
(1) d divide ambos, a e b.
(2) Se c divide a e b, então $c|d$.

A seguir, apresentamos propriedades simples do máximo divisor comum.

(*a*) $\text{mdc}(a, b) = \text{mdc}(b, a)$.

(*b*) Se $x > 0$, então $\text{mdc}(ax, bx) = x \cdot \text{mdc}(a, b)$.

(*c*) Se $d = \text{mdc}(a, b)$, então $\text{mdc}(a/b, b/d) = 1$.

(*c*) Para todo inteiro x, $\text{mdc}(a, b) = \text{mdc}(a, b + ax)$.

Algoritmo de Euclides

Sejam a e b inteiros, e seja $d = \text{mdc}(a,b)$. Sempre se pode calcular d listando todos os divisores de a e, depois, todos os divisores de b e escolhendo, então, o maior divisor comum. Fazendo $n = |a| + |b|$ e contando o número de divisões, a complexidade de tal algoritmo é $f(n) = O(\sqrt{n})$. Além disso, ainda não fornecemos um método de calcular inteiros x e y tais que

$$d = ax + by$$

Esta subseção apresenta um algoritmo muito eficiente com complexidade $f(n) = O(\log n)$ para achar $d = \text{mdc}(a, b)$ e os inteiros x e y.

Este algoritmo, denominado algoritmo de Euclides, consiste em aplicações repetidas do algoritmo de divisão. Ilustramos o algoritmo com um exemplo.

Exemplo 11.6 Seja $a = 540$ e $b = 168$. Achamos $d = \text{mdc}(a, b)$ dividindo a por b e depois, repetidamente, dividindo cada divisor pelo resto, até obter resto zero. Esses passos estão esquematizados na Figura 11-3. O último resto não nulo é 12. Logo,

$$12 = \text{mdc}\,(540, 168)$$

Isso é uma conseqüência do fato de que:

$$\text{mdc}\,(540, 168) = \text{mdc}\,(168, 36) = \text{mdc}\,(36, 24) = \text{mdc}\,(24, 12) = 12$$

$$\begin{array}{r|l} 540 & 168 \\ -504 & 3 \\ \hline 36 & \end{array} \qquad \begin{array}{r|l} 168 & 36 \\ -144 & 4 \\ \hline 24 & \end{array} \qquad \begin{array}{r|l} 36 & 24 \\ -24 & 1 \\ \hline 12 & \end{array} \qquad \begin{array}{r|l} 24 & 12 \\ -24 & 2 \\ \hline 0 & \end{array}$$

Fig. 11-3

A seguir, calculamos x e y tais que

$$12 = 540x + 168y$$

Os primeiros três quocientes da Figura 11-3 produzem as equações:

$$\begin{array}{lll} (1) & 540 = 3(168) + 36 & \text{ou} \quad 36 = 540 - 3(168) \\ (2) & 168 = 4(36) + 24 & \text{ou} \quad 24 = 168 - 4(36) \\ (3) & 36 = 1(24) + 12 & \text{ou} \quad 12 = 36 - 1(24) \end{array}$$

A equação (*3*) nos diz que 12 é uma combinação linear de 36 e 24. Usamos (*2*) para substituir 24 em (*3*) para poder escrever 12 como combinação linear de 168 e 23, como a seguir:

$$\begin{aligned} (4) \quad 12 &= 36 - 1[168 - 4(36)] = 36 - 1(168) + 4(36) \\ &= 5(36) - 1(168) \end{aligned}$$

Agora, usamos (*1*) em (*4*) para escrever 12 como combinação linear de 168 e 540 como a seguir:

$$\begin{aligned} 12 &= 5[540 - 3(168)] - 1(168) \\ &= 5(54) - 15(168) - 1(168) \\ &= 5(540) - 16(168) \end{aligned}$$

Esta é a combinação linear desejada. Logo, $x = 5$ e $y = -16$.

Mínimo Múltiplo Comum

Suponha que a e b são inteiros não nulos. Note que $|ab|$ é um múltiplo comum positivo de a e b. Logo, existe um múltiplo comum positivo mínimo de a e b; ele é representado por:

$$\text{mmc}\ (a,b)$$

e é chamado *mínimo múltiplo comum* de a e b.

Exemplo 11.7

(*a*) mmc (2, 3) = 6; mmc (4, 6) = 12; mmc (9, 10) = 90;

(*b*) Para todo inteiro positivo a, mmc $(1, a) = 1$.

(*c*) Para todo primo p e todo inteiro positivo a,

$$\text{mmc}\ (p, a) = a \qquad \text{ou} \qquad \text{mmc}\ (p, a) = ap$$

dependendo do fato de $p|a$ ou $p\nmid a$.

(*d*) Suponha que a e b são inteiros positivos. Então $a|b$ se e somente se mmc $(a, b) = b$.

O próximo teorema descreve uma relação importante entre o máximo divisor comum e o mínimo múltiplo comum.

Teorema 11-15: suponha que a e b são inteiros não nulos. Então:

$$\text{mmc}\ (a, b) = \frac{|ab|}{\text{mdc}\ (a, b)}$$

11.7 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Esta seção discute o teorema fundamental da Aritmética. Inicialmente, precisamos da noção de números relativamente primos.

Inteiros Relativamente Primos

Dois inteiros a e b são ditos relativamente primos se

$$\text{mdc}\ (a, b) = 1$$

Conseqüentemente, se a e b são relativamente primos, então existem inteiros x e y tais que

$$ax + by = 1$$

Conversamente, se $ax + by = 1$, então a e b são relativamente primos.

Exemplo 11.8

(*a*) Observe que:

$$\text{mdc}\ (12, 35) = 1, \qquad \text{mdc}\ (49, 18) = 1, \qquad \text{mdc}\ (21, 64) = 1, \qquad \text{mdc}\ (-28, 45) = 1$$

(*b*) Se p e q são primos distintos, então mdc$(p, q) = 1$.

(*c*) Para qualquer inteiro a, temos

$$\text{mdc}\ (a, a + 1) = 1$$

Isso decorre de que qualquer divisor comum de a e $a + 1$ deve dividir a diferença $a + 1 - a = 1$.

A relação descrita pela propriedade de números serem relativamente primos é particularmente importante devido aos resultados enunciados a seguir. Provaremos o segundo teorema.

Teorema 11-16: suponha que mdc$(a, b) = 1$ e que ambos a e b dividem c. Então, ab divide c.

Teorema 11-17: suponha que $a|bc$ e que mdc$(a, b) = 1$. Então, $a|c$.

Demonstração: Como $\text{mdc}(a, b) = 1$, existem x e y tais que $ax + by = 1$. Multiplicando por c, obtém-se:

$$acx + bcy = c$$

Sabemos que $a|acx$. Além disso, $a|bcy$ já que, por hipótese, $a|bc$. Portanto, a divide a soma $acx + bcy = c$.

Corolário 11-18: suponha que um primo p divide um produto ab. Então, $p|a$ ou $p|b$.

Esse corolário remonta aos tempos de Euclides. De fato, ele é a base da demonstração do Teorema Fundamental da Aritmética.

O Teorema Fundamental da Aritmética

O Teorema 11.10 afirma que todo inteiro positivo é um produto de primos. Será que produtos distintos de primos podem gerar o mesmo número? Claramente, podemos reordenar os fatores primos, por exemplo,

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 5$$

O Teorema Fundamental da Aritmética (demonstrado no Problema 11.35) afirma que essa é a única forma de dois produtos "distintos" resultarem no mesmo número. Enunciamos:

Teorema 11-19: **(Teorema Fundamental da Aritmética)** todo inteiro $n > 1$ pode ser expresso de maneira única (exceto pela ordem) como um produto de primos.

Os primos na fatoração de n não precisam ser distintos. Freqüentemente, é útil manter juntos os primos iguais. Neste caso, n pode ser expresso de maneira única na forma:

$$n = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

onde os m_i são positivos e $p_1 < p_2 < \cdots < p_r$. Essa forma é conhecida como *fatoração canônica* de n.

Exemplo 11.9 Sejam $a = 2^4 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13$ e $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 17$. Ache $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$.

(*a*) Primeiramente achamos $\text{mdc}(a, b)$. Os primos p_i que aparecem em ambos a e b, i.e., 2, 3 e 11, também aparecerão em d, e o expoente de p_i em d será o menor dos expoentes que aparecem em a e b. Logo,

$$d = \text{mdc}(a, b) = 2^3 \cdot 3^2 \cdot 11 = 792$$

(*b*) Depois, achamos $m = \text{mmc}(a, b)$. Os primos p_i que aparecem em a ou b, i.e., 2, 3, 5, 7, 11, 13 e 17 também vão aparecer em m, e o expoente de p_i em m será o maior expoente que aparece nas fatorações de a e b. Logo,

$$m = \text{mmc}(a, b) = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17$$

Estamos tão acostumados a usar os números como se o Teorema Fundamental da Aritmética fosse verdadeiro que pode nos parecer que ele não necessita demonstração. Devemos tributar a Euclides, que primeiro o provou, o reconhecimento da necessidade de sua demonstração. Enfatizamos que o teorema não é trivial apresentando um exemplo de um sistema de números que não satisfaz o teorema.

Exemplo 11.10 Seja F o conjunto de inteiros positivos da forma $3x + 1$. Logo, F consiste nos números

$$1, \quad 4, \quad 7, \quad 10, \quad 13, \quad 16, \quad 19, \quad 22, \ldots$$

Note que o produto de dois números em F também pertence a F, pois

$$(3x + 1)(3y + 1) = 9xy + 3x + 3y + 1 = 3(3xy + x + y) + 1$$

Nossa definição de primos faz total sentido em F. Os primeiros primos são:

$$4, \quad 7, \quad 10, \quad 13, \quad 19, \quad 22, \quad 25, \ldots$$

Embora $4 = 2 \cdot 2$, o número 2 não está em F. Portanto, 4 é um primo em F, já que 4 não tem fatores, exceto 1 e 4. De modo análogo, 10, 22, 25... são primos em F. Note que $100 = 3(33) + 1$ pertence a F. Entretanto, 100 tem, essencialmente, duas diferentes fatorações com primos em F; a saber:

$$100 = 4 \cdot 25 \quad \text{e} \quad 100 = 10 \cdot 10$$

Portanto, não existe uma fatoração única de primos em F.

11.8 RELAÇÃO DE CONGRUÊNCIA

Seja m um inteiro positivo. Dizemos que a *é congruente* a b *módulo* m, denotado por

$$a \equiv b \text{ (modulo } m) \qquad \text{ou simplesmente} \qquad a \equiv b \text{ (mod } m)$$

Se m divide a diferença $a - b$. O inteiro m é dito o *modulus*. A negação de $a \equiv b \pmod m$ é descrita por $a \not\equiv b \pmod m$. Por exemplo:

(i) $87 \equiv 23 \pmod 4$, pois 4 divide $87 - 23 = 64$.

(ii) $67 \equiv 1 \pmod 6$, pois 6 divide $67 - 1 = 66$.

(iii) $72 \equiv -5 \pmod 7$, pois 7 divide $72 - (-5) = 77$.

(iv) $27 \not\equiv 8 \pmod 9$ pois 9 não divide a diferença $27 - 8 = 19$.

Nosso primeiro teorema (demonstrado no Problema 11.40), afirma que congruência módulo m é uma relação de equivalência.

Teorema 11-20: seja m um inteiro positivo. Então:

(i) Para todo inteiro a, $a \equiv a \pmod m$.

(ii) Se $a \equiv b \pmod m$, então $b \equiv a \pmod m$.

(iii) Se $a \equiv b \pmod m$ e $b \equiv c \pmod m$, então $a \equiv c \pmod m$.

Observação: Suponha que m é positivo e que a é um inteiro qualquer. Pelo Algoritmo de Divisão, existem inteiros q e r, com $0 \le r \le m$, tais que $a = mq + r$. Portanto,

$$mq = a - r \qquad \text{ou} \qquad m|(a - r) \qquad \text{ou} \qquad a \equiv r \pmod m$$

Conseqüentemente,

(1) Todo inteiro a é congruente módulo m a um único inteiro no conjunto

$$\{0, 1, 2, \ldots, m - 1\}$$

A unicidade é conseqüência do fato de que m não pode dividir a diferença de dois inteiros no conjunto.

(2) Dois inteiros quaisquer, a e b, são congruentes módulo m se os restos da divisão de cada um deles por m coincidem.

Classes de Resíduos

Como congruência módulo m é uma relação de equivalência, ela induz uma partição em classes de equivalência disjuntas – chamadas *classes de resíduo módulo* m – no conjunto $\mathbf{Z}$ dos inteiros. Pelas observações acima, uma classe de equivalência módulo m consiste em todos os inteiros que, quando divididos por m, produzem o mesmo resto. Portanto, existem m classes de resíduo e cada uma delas contém exatamente um dos inteiros no conjunto de restos possíveis,

$$\{0, 1, \ldots, m - 1\}$$

Em geral, um conjunto de m inteiros $\{a_1, a_2, \ldots, a_m\}$ é dito um *sistema completo de resíduos módulo* m se cada a_i vem de uma classe de resíduos distinta. Logo, os inteiros de 0 a $m - 1$ formam um sistema completo de resíduos. De fato, quaisquer m inteiros consecutivos formam um sistema completo de resíduos módulo m.

A notação $[x]_m$, ou simplesmente $[x]$, é usada para denotar a classe de resíduos (módulo m) que contém um inteiro x, isto é, os inteiros congruentes a x. Em outras palavras,

$$[x] = \{a \in \mathbf{Z}: a \equiv x \pmod m\}$$

Conseqüentemente, as classes de resíduos podem ser denotadas por

$$[0], \quad [1], \quad [2], \quad \ldots, \quad [m - 1]$$

ou usando qualquer outra escolha de inteiros em um sistema de resíduos completo.

Hidden page

Inteiros Módulo m, Z_m

Os *inteiros módulo m*, denotados por Z_m, formam o conjunto

$$\mathbf{Z}_m = \{0, 1, 2, 3, \ldots, m-1\}$$

onde adição e multiplicação são definidas pela aritmética módulo m ou, em outras palavras, pelas operações correspondentes nas classes de resíduos. Por exemplo, a Figura 11-14 também pode ser vista como sendo a tabela de adição e multiplicação de Z_6. Isso significa que:

> Não existe diferença essencial entre Z_m e a aritmética das classes de resíduo módulo m e, portanto, ambos serão tratados indistintamente.

Leis de Cancelamento para Relações de Congruência

Lembre que os inteiros satisfazem a seguinte lei:

> Lei do cancelamento: se $ab = ac$ e $a \neq 0$, então $b = c$.

A diferença crucial entre a aritmética comum e a aritmética módulo m é que a lei de cancelamento acima é falsa para relações de congruência. Por exemplo,

$$3 \cdot 1 \equiv 3 \cdot 5 \pmod 6 \qquad \text{mas} \qquad 1 \not\equiv 5 \pmod 6$$

Isto é, não podemos cancelar 3, ainda que $3 \not\equiv 0 \pmod 6$. Entretanto, temos a seguinte *lei do cancelamento modificada* para as relações de congruência.

Teorema 11-22: **(Lei do cancelamento modificada)** suponha $ab \equiv bc \pmod m$ e $\text{mdc}(a, m) = 1$. Então, $b \equiv c \pmod m$.

O teorema acima é uma conseqüência do seguinte resultado geral (demonstrado no Problema 11.44):

Teorema 11-23: suponha que $ab \equiv bc \pmod m$ e $d = \text{mdc}(a, m)$. Então, $b \equiv c \pmod{m/d}$.

Exemplo 11.13 Considere a congruência seguinte:

$$6 \equiv 36 \pmod{10} \tag{1}$$

Como 3 e o *modulus* 10 são relativamente primos, podemos dividir ambos os lados de (1) por 3 para obter

$$2 \equiv 12 \pmod{10}$$

Observe que não podemos dividir ambos os lados de (1) por 6; isto é,

$$1 \not\equiv 6 \pmod{10}$$

Entretanto, pelo Teorema 11.23, podemos dividir ambos os lados de (1) por 6 se também dividirmos o *modulus* por $2 = \text{mdc}(6,10)$. Isto é,

$$1 \equiv 6 \pmod 5$$

Observação: Suponha que p é um primo. Então, os inteiros de 1 até $p - 1$ são relativamente primos a p. Portanto, vale a lei de cancelamento usual quando um *modulus* é um primo p. Isto é,

> Se $ab \equiv ac \pmod p$ e $a \not\equiv 0 \pmod p$, então $b \equiv c \pmod p$.

Portanto, $\mathbf{Z}_p$, os inteiros módulo um primo p, desempenham um papel importante na teoria dos números.

Sistemas de Resíduos Reduzidos, Função Phi de Euler

A lei do cancelamento modificada, Teorema 11.22, é indicativa do papel especial desempenhado pelos inteiros relativamente primos com o *modulus* m. Observamos que a é um primo relativo de m se e somente se todo elemento na classe de resíduos $[a]$ é relativamente primo a m. Portanto, podemos falar de uma classe de resíduos que é relativamente prima com m.

O número de classes de resíduos relativamente primas com m, ou, equivalentemente, o número de inteiros entre 1 e m (inclusive) primos relativos de m, é denotado por

$$\phi(m)$$

A função $\phi(m)$ é dita a *função Phi de Euler*. A lista de números entre 1 e m que são primos relativos a m, ou, mais geralmente, qualquer lista $\phi(m)$ de inteiros não congruentes que são primos relativos de m, é dita um *sistema de resíduos reduzido módulo m*.

Exemplo 11.14

(*a*) Considere o *modulus* $m = 15$. Existem oito inteiros entre 1 e 15 que são primos relativos de 15:

$$1, \quad 2, \quad 4, \quad 7, \quad 8, \quad 11, \quad 13, \quad 14$$

Logo, $\phi(15) = 8$, e os oito inteiros acima formam um sistema reduzido de resíduos módulo 15.

(*b*) Considere qualquer primo p. Todos os números $1, 2, \ldots, p-1$ são primos relativos de p; logo, $\phi(p) = p - 1$.

Uma função f com domínio nos inteiros positivos $\mathbf{N}$ é dita multiplicativa se, para todo a e b relativamente primos,

$$f(ab) = f(a)\, f(b)$$

Vale o teorema seguinte (demonstrado no Problema 11.51).

Teorema 11-24: a função Phi de Euler é multiplicativa. Isto é, se a e b são primos relativos, então,

$$\phi(ab) = \phi(a)\phi(b).$$

11.9 EQUAÇÕES DE CONGRUÊNCIA

Uma *equação polinomial de congruência* ou, simplesmente, uma *equação de congruência* (em uma incógnita x) é uma equação da forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{m} \qquad (*)$$

Uma tal equação é dita de *grau n* se $a_n \not\equiv 0 \pmod{m}$.

Suponha $s \not\equiv t \pmod{m}$. Então s é uma solução de $(*)$ se e somente se t é uma solução de $(*)$. Portanto, o *número de soluções* de $(*)$ é definido como o número de soluções não congruentes ou, equivalentemente, o número de soluções no conjunto

$$\{0, 1, 2, \ldots, m-1\}$$

Obviamente, essas soluções podem ser sempre achadas por substituição direta de cada um dos m números em $(*)$ para verificar se, de fato, satisfazem a equação.

O *conjunto completo de soluções* de $(*)$ é um conjunto maximal de soluções não congruentes, enquanto a *solução geral* de $(*)$ é o conjunto de todas as soluções de $(*)$. A solução geral pode ser achada adicionando todos os múltiplos do *modulus* m a qualquer conjunto completo de soluções.

Exemplo 11.15 Considere as equações:

(*a*) $x^2 + x + 1 \equiv 0 \pmod{4}$.

(*b*) $x^2 + 3 \equiv 0 \pmod{6}$.

(*c*) $x^2 - 1 \equiv 0 \pmod{8}$.

Achamos aqui a solução por testes.

(*a*) Não existe solução, pois 0, 1, 2 e 3 não satisfazem a equação.

(*b*) Existe apenas uma solução entre 0, 1,..., 5 que é 3. Portanto, a solução geral consiste nos inteiros $3 + 6k$, onde $k \in \mathbf{Z}$.

(*c*) Existem quatro soluções, 1, 3, 5 e 7. Isso mostra que uma equação de congruência de grau n pode ter mais de n soluções.

Enfatizamos que não estamos interessados apenas no estudo de equações de congruência para achar suas soluções; isso pode ser feito por meio de testes. Estamos interessados principalmente no desenvolvimento de técnicas que auxiliem a achar as soluções e em uma teoria que nos diga o número de soluções e sob que condições existem. Existe uma teoria como esta para equações de congruência lineares, que investigamos a seguir. Também discutimos o teorema chinês do resto, que é, essencialmente, um sistema de congruência lineares.

Observação 1: Os coeficientes de uma equação de congruência podem ser reduzidos módulo m, pois isto resulta em uma *equação equivalente*, isto é, uma equação com as mesmas soluções. Por exemplo,

$$15x^2 + 28x + 14 \equiv 0 \pmod 6, \qquad 3x^2 + 4x + 2 \equiv 0 \pmod 6, \qquad 3x^2 - 2x + 2 \equiv 0 \pmod 6,$$

são equações equivalentes, já que os seus coeficientes são congruentes mod $m = 6$. Normalmente escolhemos coeficientes entre 0 e $m - 1$ ou entre $-m/2$ e $m/2$.

Observação 2: Como, na verdade, estamos procurando soluções de $(*)$ nas classes de equivalência módulo m e não no conjunto dos inteiros, podemos considerar $(*)$ como uma equação sobre $\mathbf{Z}_m$, os inteiros módulo m, e não como uma equação sobre $\mathbf{Z}$, os inteiros. Neste contexto, o número de soluções de $(*)$ é simplesmente o número de soluções em $\mathbf{Z}_m$.

Equação de Congruência Linear: $ax \equiv 1 \pmod m$

Consideramos primeiramente uma equação especial

$$ax \equiv 1 \pmod m \qquad (**)$$

onde $a \not\equiv 0 \pmod m$. A história completa desta equação é dada pelo seguinte teorema (demonstrado no Problema 11.65).

Teorema 11-25: se a e m são primos relativos, então $ax \equiv 1 \pmod m$ tem solução única; caso contrário, não há solução.

Exemplo 11.16

(*a*) Considere a equação de congruência

$$6x \equiv 1 \pmod{33}$$

Observe que o mdc(6, 33) = 3. Logo, a equação não tem solução.

(*b*) Considere a equação de congruência

$$7x \equiv 1 \pmod 9$$

Aqui, o mdc(7, 9) = 1; logo, a equação tem solução única. Testando os números 0,1,.., 8, concluímos que

$$7(4) = 28 \equiv 1 \pmod 9$$

Logo, $x = 4$ é a nossa solução única. (A solução geral é $4 + 9k$ para $k \in \mathbf{Z}$.)

Suponha que exista uma solução de $(**)$, isto é, suponha que $\text{mdc}(a, m) = 1$, e suponha que o *modulus* m seja grande. Então, o algoritmo de Euclides pode ser usado para achar a solução de $(**)$. Especificamente, usamos o algoritmo de Euclides para determinar x_0 e y_0 tais que

$$ax_0 + my_0 = 1$$

de onde se conclui que $ax_0 \equiv 1 \pmod m$; isto é, x_0 é solução de $(**)$.

Hidden page

A história completa do caso geral de $(***)$ está contida no teorema seguinte (demonstrado no Problema 11.67).

Teorema 11-27: considere a equação $a \equiv b \pmod{m}$ onde $D = \text{mdc}(a, m)$.

(i) Suponha que d não divide b. Então $ax \equiv b \pmod{m}$ não tem solução.

(ii) Suponha que d divide b. Então $ax \equiv b \pmod{m}$ tem d soluções que são todas congruentes módulo M à única solução de

$$Ax \equiv B \pmod{M}$$

Onde $A = a/d$, $B = b/d$ e $M = m/d$.

Observe que o Teorema 11.26 se aplica à equação $Ax \equiv B \pmod{M}$ no Teorema 11.27, pois $\text{mdc}(A, M) = 1$.

Exemplo 11.19 Resolva cada equação de congruência: (*a*) $4x \equiv 9 \pmod{14}$, (*b*) $8x \equiv 12 \pmod{28}$.

(*a*) Note que $\text{mdc}(4, 14) = 2$. Entretanto, 2 não divide 9. Logo, a equação não tem solução.

(*b*) Note que $d = \text{mdc}(8, 28) = 4$, e $d = 4$ divide 12. Logo, a equação tem $d = 4$ soluções. Dividindo cada termo na equação por $d = 4$, obtemos a equação de congruência

$$2x \equiv 3 \pmod{7} \qquad (1)$$

que tem solução única. Testando os inteiros 0, 1,..., 6, concluímos que 5 é a solução única de (*1*). Agora somamos até $d - 1 = 3$ múltiplos de 7 à solução 5 de (*1*) obtendo:

$$5 + 7 = 12, \qquad 5 + 2(7) = 19, \qquad 5 + 3(7) = 26$$

Conseqüentemente, 5, 12, 19, 26 são as $d = 4$ soluções da equação original (*b*).

Observação: A solução da equação (*1*) no Exemplo 11.19 foi obtida por inspeção. Entretanto, quando o *modulus m* é grande, sempre se pode usar o algoritmo de Euclides para achar a única solução como no Exemplo 11.17. (Veja o Problema 11.61.)

Teorema Chinês do Resto

Um velho mago chinês fez a seguinte pergunta:

> Existe um inteiro positivo x tal que quando x é dividido por 3 dá resto 2, quando x é dividido por 5, dá resto 4, e quando x é dividido por 7 dá resto 6?

Em outras palavras, procuramos uma solução comum para as três seguintes equações de congruência:

$$x \equiv 2 \pmod{3}, \qquad x \equiv 4 \pmod{5}, \qquad x \equiv 6 \pmod{7}$$

Observe que os módulos 3, 5 e 7 são, dois a dois, primos relativos. Logo, podemos usar o teorema a seguir; ele nos diz que existe uma solução única módulo $M = 3 \cdot 5 \cdot 7 = 105$.

Teorema 11-28: **(Teorema Chinês do Resto)** considere o sistema

$$x \equiv r_1 \pmod{m_1}, \qquad x \equiv r_2 \pmod{m_2}, \qquad \ldots, \qquad x \equiv r_k \pmod{m_k} \qquad (*)$$

onde os m_i são, dois a dois, primos relativos. Então, o sistema tem uma única solução módulo $M = m_1 m_2 \cdots m_k$.

De fato, pode-se dar uma fórmula explícita (apresentada na proposição seguinte) para a solução do sistema $(*)$ no Teorema 11.28.

Proposição 11.29: Considere o sistema $(*)$ de equações de congruência. Seja $M = m_1 m_2 \cdots m_k$ e

$$M_1 = \frac{M}{m_1}, \qquad M_2 = \frac{M}{m_2}, \qquad \ldots, \qquad M_k = \frac{M}{m_k}$$

(Então, M_i e m_i são primos relativos para cada i.) Sejam $s_1, s_2, \ldots, s_k$ soluções, respectivamente, das equações de congruência

$$M_1 x \equiv 1 \pmod{m_1}, \quad M_2 x \equiv 1 \pmod{m_2}, \quad \cdots \quad M_k x \equiv 1 \pmod{m_k}$$

Então,

$$X_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k \qquad (**)$$

É uma solução do sistema $(*)$.

Agora, resolvemos o enigma original de duas maneiras.

Método 1: Primeiramente aplicamos o teorema às duas primeiras equações,

$$(a) \quad x \equiv 2 \pmod 3 \qquad \text{e} \qquad (b) \quad x \equiv 4 \pmod 5$$

Pelo teorema, existe uma única solução módulo $M = 3 \cdot 5 = 15$. Adicionando múltiplos do *modulus* $m = 5$ à solução dada $x = 4$ da segunda equação (b), obtemos as três soluções seguintes de (b), que são menores do que 15;

$$4, \quad 9, \quad 14$$

Testando cada uma destas soluções na equação (a), achamos que 14 é a única solução de ambas as equações.

Agora aplicamos o mesmo processo às duas equações

$$(c) \quad x \equiv 14 \pmod{15} \qquad \text{e} \qquad (d) \quad x \equiv 6 \pmod 7$$

Pelo teorema, existe uma única solução módulo $M = 15 \cdot 7 = 105$. Somando múltiplos do módulo $m = 15$ à solução dada $x = 14$ da primeira equação (c), obtemos as seguintes sete soluções de (b) que são menores do que 105:

$$14, \quad 29, \quad 44, \quad 59, \quad 74, \quad 89, \quad 104$$

Testando cada uma destas soluções de (c) na segunda equação (d), achamos que 104 é a única solução de ambas as equações. Logo,

$$x = 104$$

é o menor inteiro positivo que satisfaz as três equações, isto é, que é a solução do enigma.

Método 2: Usando a notação acima, obtemos

$$M = 3 \cdot 5 \cdot 7 = 105, \qquad M_1 = 105/3 = 35, \qquad M_2 = 105/5 = 21, \qquad M_3 = 105/7 = 15$$

Procuramos agora soluções para as equações

$$35x \equiv 1 \pmod 3, \qquad 21x \equiv 1 \pmod 5, \qquad 15x \equiv 1 \pmod 7$$

Reduzindo 35 módulo 3, reduzindo 21 módulo 5, e reduzindo 15 módulo 7, obtemos o sistema

$$2x \equiv 1 \pmod 3, \qquad x \equiv 1 \pmod 5, \qquad x \equiv 1 \pmod 7$$

As soluções dessas três equações são, respectivamente,

$$s_1 = 2, \qquad s_2 = 1, \qquad s_3 = 1$$

Agora substituímos na fórmula $(**)$ para obter as seguintes soluções do sistema original:

$$x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 4 + 15 \cdot 1 \cdot 6 = 314$$

Dividindo essa solução pelo *modulus* $M = 105$, obtemos o resto

$$x = 104$$

que é a única solução do enigma entre 0 e 105.

Observação: As soluções $s_1 = 2, s_2 = 1, s_3 = 1$ foram obtidas por inspeção. Se os *moduli*[†] forem grandes, sempre se pode usar o algoritmo de Euclides para achar as soluções como no Exemplo 11.17.

Problemas Resolvidos

Inequações, Valor Absoluto

11.1 Insira o símbolo correto, $<$, $>$ ou $=$, entre cada par de inteiros:

(*a*) $4 \_\_\_\_ -7$, (*c*) $3^2 \_\_\_\_ 5$, (*e*) $3^2 \_\_\_\_ 9$

(*b*) $-2 \_\_\_\_ -9$, (*d*) $-8 \_\_\_\_ 3$, (*f*) $6 \_\_\_\_ 8$

Para cada par de inteiros, a e b, determine suas posições relativas na reta $\mathbf{R}$; ou compute $b - a$ e escreva

$$a < b, \qquad a > b \qquad \text{ou} \qquad a = b$$

dependendo de $b - a$ ser positivo, negativo ou zero. Portanto,

(*a*) $4 > -7$; (*b*) $-2 > -9$; (*c*) $3^2 > 5$; (*d*) $-8 < 3$; (*e*) $3^2 = 9$, (*f*) $6 < 8$.

11.2 Avalie: (*a*) $|-4|$, $|3|$, $|0|$; (*b*) $|2-5|$, $|-2+5|$, $|-2-5|$; (*c*) $|5-8|+|2-4|$, $|4-3|-|3-9|$.

(*a*) O valor absoluto é a "magnitude" do número, desconsiderando o sinal. Logo,

$$|-4| = 4, \qquad |3| = 3, \qquad |0| = 0$$

(*b*) Avalie dentro dos delimitadores do módulo primeiramente:

$$|2-5| = |-3| = 3, \qquad |-2+5| = |3| = 3, \qquad |-2-5| = |-7| = 7$$

(*c*) Avalie dentro dos delimitadores do módulo primeiramente:

$$|5-8| + |2-4| = |-3| + |-2| = 3 + 2 = 5$$

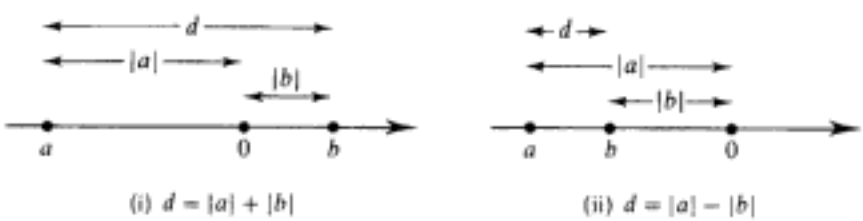
$$|4-3| - |3-9| = |1| - |-6| = 1 - 6 = -5$$

11.3 Ache a distância d entre cada par de inteiros:

(*a*) 3 e –7; (*b*) –4 e 2; (*c*) 1 e 9; (*d*) –8 e –3; (*e*) 4 e –4; (*f*) –5 e –8.

A distância d entre a e b é dada por $d = |a-b| = |b-a|$. Opcionalmente, como indicado na Figura 11-5, $d = |a| + |b|$ quando a e b têm sinais diferentes, e $d = |a| - |b|$ se a e b têm o mesmo sinal e $|a| \geq |b|$.

Logo: (*a*) $d = 3 + 7 = 10$; (*b*) $d = 4 + 2 = 6$; (*c*) $d = 9 - 1 = 8$; (*d*) $d = 8 - 3 = 5$; (*e*) $d = 4 + 4 = 8$; (*f*) $d = 8 - 5 = 3$.



(i) $d = |a| + |b|$ (ii) $d = |a| - |b|$

Fig. 11-5

[†] N. de R. Do latim, plural de *modulus*.

11.4 Determine todos os inteiros n tais que: (*a*) $1 < 2n - 6 < 14$; (*b*) $2 < 8 - 3n < 18$.

(*a*) Adicione 6 aos "três lados" para obter $7 < 2n < 20$. Depois, divida todos os lados por 2 (ou multiplique por $\frac{1}{2}$) para obter $3{,}5 < n < 10$. Logo,

$$n = 4, 5, 6, 7, 8, 9$$

(*b*) Adicione –8 aos três lado para obter $-6 < -3n < 10$. Divida todos por –3 e, como –3 é negativo, mude a direção da desigualdade para obter

$$2 > n > -3{,}3 \qquad \text{ou} \qquad -3{,}3 < n < 2$$

Logo, $n = -3, -2, -1, 0, 1$.

11.5 Prove a Proposição 11.1 (iii): se $a \leq b$ e $b \leq c$, então $a \leq c$.

A proposição é obviamente verdadeira quando $a = b$ e $b = c$. Portanto, precisamos considerar apenas o caso $a < b$ e $b < c$. Logo, $b - a$ e $c - b$ são positivos. Logo, pela propriedade $[\mathbf{P}_1]$ dos inteiros positivos $\mathbf{N}$, a soma também é positiva. Isto é,

$$(b - a) + (c - b) = c - a$$

é positivo. Logo, $a < c$ de onde se conclui, $a \leq c$.

11.6 Prove a Proposição 11.3: suponha que $a \leq b$, e suponha que c é um inteiro qualquer. Então:
(i) $a + c \leq b + c$, (ii) $ac \leq bc$ se $c > 0$ e $ac \geq bc$ se $c < 0$.

A proposição é certamente verdade se $a = b$. Logo, só precisamos considerar o caso de $a < b$, isto é, $b - a$ é positivo.

(i) A seguinte diferença é positiva:

$$(b + c) - (a + c) = b - a$$

Logo, $a + c < b + c$.

(ii) Suponha que c é positivo. Pela propriedade $[\mathbf{P}_1]$ dos inteiros positivos $\mathbf{N}$, o seguinte produto também é positivo:

$$c(b - a) = bc - ac$$

Logo, $ac < bc$. Agora, suponha que c é negativo. Logo, $-c$ é positivo, e o produto seguinte também é positivo:

$$(-c)(b - a) = ac - bc$$

Conseqüentemente, $bc < ac$, e, portanto, $ac > bc$.

11.7 Prove a Proposição 11.4 (iii): $|ab| = |a|\,|b|$.

A demonstração consiste em analisar caso por caso.

(*a*) Suponha que $a = 0$ ou $b = 0$.

Então, $|a| = 0$ ou $|b| = 0$ e, logo, $|a||b| = 0$. Além disso, $ab = 0$. Portanto,

$$|ab| = 0 = |a|\,|b|$$

(*b*) Suponha que $a > 0$ e $b > 0$.

Então, $|a| = a$ e $|b| = b$. Logo,

$$|ab| = ab = |a|\,|b|$$

(*c*) Suponha que $a > 0$ e $b < 0$.

Então, $|a| = a$ e $|b| = -b$. Além disso, $ab < 0$. Logo,

$$|ab| = -(ab) = a(-b) = |a|\,|b|$$

(*d*) Suponha que $a < 0$ e $b > 0$.

Então, $|a| = -a$ e $|b| = b$. Além disso, $ab < 0$. Logo,

$$|ab| = -(ab) = (-a)b = |a|\,|b|$$

Hidden page

Hidden page

11.14 Prove o Teorema 11.6 (princípio da boa ordenação): seja S um conjunto não vazio de inteiros positivos. Então, S contém um elemento mínimo.

Suponha que S não tem um elemento mínimo. Seja M o conjunto dos inteiros positivos que são menores do que qualquer elemento de S. Então, $1 \in M$; caso contrário, $1 \in S$ e 1 seria um elemento mínimo de S. Suponha que $k \in M$. Então k é menor do que todo elemento de S. Portanto, $k + 1 \in M$; caso contrário, $k + 1$ seria o menor elemento de S.

Pelo princípio da indução matemática, M contém todo inteiro positivo. Logo, S é vazio. Isso contradiz a hipótese de que S é não vazio. Conseqüentemente, a hipótese original de que S não contém um elemento mínimo não é verdade. Logo, o teorema é verdade.

11.15 Prove o Teorema 11.5 (indução: segunda forma): seja P uma proposição definida nos inteiros $n \geq 1$ tal que:

(i) $P(1)$ é verdade.

(ii) $P(n)$ é verdade sempre que $P(k)$ é verdade para todo $1 \leq k < n$. Então P é verdade para todo $n \geq 1$.

Seja A o conjunto dos inteiros $n \geq 1$ para os quais P não é verdade. Suponha que A não é vazio. Pelo princípio da boa ordenação, A contém um elemento mínimo a_0. Por (i), $a_0 \neq 1$.

Como a_0 é o menor elemento de A, P é verdade para todo inteiro k onde $1 \leq k < a_0$. Por (ii), P é verdade para a_0.

Isso contradiz o fato de $a_0 \in A$. Logo, A é vazio, e, portanto, P é verdade para todo inteiro $n \geq 1$.

Algoritmo de Divisão

11.16 Para cada par de inteiros a e b, ache inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$:

$$(a)\ a = 258 \quad \text{e} \quad b = 12; \quad (b)\ a = 573 \quad \text{e} \quad b = -16.$$

(*a*) Aqui, a e b são positivos. Apenas divida a por b, isto é, 258 por 12, como na Figura 11-6(*a*). Então, $q = 21$ e $r = 6$.

(*b*) Aqui, a é positivo, mas b é negativo. Divida a por $|b|$, isto é, 573 por 16, como na Figura 11-6(*b*). Então:

$$573 = (16)(35) + 13 = 573 = (-16)(-35) + 13$$

Logo, $q = -35$ e $r = 13$.

$$\begin{array}{r|l} 258 & 12 \\ -24 & 21 \\ \hline 18 & \\ -12 & \\ \hline 6 & \end{array} \qquad \begin{array}{r|l} 573 & 16 \\ -48 & 35 \\ \hline 93 & \\ -80 & \\ \hline 13 & \end{array} \qquad \begin{array}{r|l} 381 & 14 \\ -28 & 27 \\ \hline 101 & \\ -98 & \\ \hline 3 & \end{array} \qquad \begin{array}{r|l} 433 & 17 \\ -34 & 25 \\ \hline 93 & \\ -85 & \\ \hline 8 & \end{array}$$

(*a*) (*b*) (*c*) (*d*)

Fig. 11-6

11.17 Para cada par de inteiros a e b, ache inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$:

$$(a)\ a = -381 \quad \text{e} \quad b = 14; \quad (b)\ a = -433 \quad \text{e} \quad b = -17.$$

Aqui, a é negativo em todos os casos e, portanto, precisamos fazer alguns ajustes para garantir que $0 \leq r < |b|$.

(*a*) Divida $|a| = 381$ por $b = 14$, como na Figura 11-6(*c*). Então,

$$381 = (14)(27) + 3 \qquad \text{e, portanto,} \qquad -381 = (14)(-27) - 3$$

Mas –3 é negativo e não pode ser o resto r; logo, somamos e subtraímos $b = 14$ como a seguir:

$$-381 = (14)(-27) - 14 + 14 - 3 = (14)(-28) + 11$$

Logo, $q = -28$ e $r = 11$.

(*b*) Divida $|a| = 433$ por $|b| = 17$, como na Figura 11-6(*d*). Logo,

$$433 = (17)(25) + 8 \qquad \text{e, portanto,} \qquad -433 = (-17)(25) - 8$$

Hidden page

11.21 Prove o Teorema 11.7 (algoritmo de divisão): sejam a e b são inteiros com $b \neq 0$. Então existem inteiros q e r tais que

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < |b|$$

Além disso, os inteiros q e r são únicos.

Seja M o conjunto dos inteiros não negativos da forma $a - xb$ para algum inteiro x. Se $x = -|a|b$ então $a - xb$ é não negativo (Problema 11.78); logo, M é não vazio. Pelo princípio da boa ordenação, M tem um elemento mínimo, digamos, r. Como $r \in M$, temos

$$r \geq 0 \qquad \text{e} \qquad r = a - qb$$

para algum inteiro q. Precisamos mostrar apenas que inteiro $r < |b|$. Suponha que $r \geq |b|$. Seja $r' = r - |b|$. Então, $r' \geq 0$ e $r' < r$ porque $b \neq 0$. Além disso,

$$r' = r - |b| = a - qb - |b| = \begin{cases} a - (q+1)b, & \text{if } b < 0 \\ a - (q-1)b, & \text{if } b > 0 \end{cases}$$

Em qualquer caso, r' pertence a M. Isso contradiz o fato de que r é elemento mínimo de M. Conseqüentemente, $r < |b|$. Logo, a existência de q e r está provada.

Agora, mostraremos a unicidade de q e r. Suponha que existem inteiros q e r e q' e r' tais que

$$a = bq + r \qquad \text{e} \qquad a = bq' + r' \qquad \text{e} \qquad 0 \leq r, r' < |b|$$

Então, $bq + r = bq' + r'$; portanto,

$$b(q - q') = r' - r$$

Logo, b divide $r' - r$. Mas $|r' - r| < |b|$, já que $0 \leq r, r' < |b|$. Conseqüentemente, $r' - r = 0$. Isso implica $q - q' = 0$, já que $b \neq 0$. Conseqüentemente, $r' = r$ e $q' = q$; isto é, q e r são unicamente determinados por a e b.

Divisibilidade, Primos, Máximo Divisor Comum

11.22 Ache todos os divisores positivos de: (*a*) 18; (*b*) $256 = 2^8$; (*c*) $392 = 2^3 \cdot 7^2$.

(*a*) Como 18 é relativamente pequeno, simplesmente escrevemos todos os inteiros positivos (≤ 18) que dividem 18. São:

$$1, \quad 2, \quad 3, \quad 6, \quad 9, \quad 18$$

(*b*) Como 2 é primo, os divisores positivos de $256 = 2^8$ são as potências menores de 2, i.e.,

$$2^0, \quad 2^1, \quad 2^2, \quad 2^3, \quad 2^4, \quad 2^5, \quad 2^6, \quad 2^7, \quad 2^8$$

Em outras palavras, os divisores de 256 são

$$1, \quad 2, \quad 4, \quad 8, \quad 16, \quad 32, \quad 64, \quad 128, \quad 256$$

(*c*) Como 2 e 7 são primos, os divisores positivos de $392 = 2^3 \cdot 7^2$ são produtos de potências mais baixas de 2 vezes potências mais baixas de 7, i.e.,

$$2^0 \cdot 7^0, \quad 2^1 \cdot 7^0, \quad 2^2 \cdot 7^0, \quad 2^3 \cdot 7^0, \quad 2^0 \cdot 7^1, \quad 2^1 \cdot 7^1, \quad 2^2 \cdot 7^1, \quad 2^3 \cdot 7^1,$$
$$2^0 \cdot 7^2, \quad 2^1 \cdot 7^2, \quad 2^2 \cdot 7^2, \quad 2^3 \cdot 7^2$$

Em outras palavras, os divisores positivos de 392, são

$$1, \quad 2, \quad 4, \quad 8, \quad 7, \quad 14, \quad 28, \quad 56, \quad 49, \quad 98, \quad 196, \quad 392.$$

(Usamos a convenção usual de que $n^0 = 1$ para qualquer n não nulo.)

11.23 Liste todos os primos entre 50 e 100.

Simplesmente, liste todos os números p entre 50 e 100 que não podem ser escritos como produto de dois inteiros positivos, excluindo 1 e p. Isto produz:

$$51, \quad 53, \quad 57, \quad 59, \quad 61, \quad 67, \quad 71, \quad 73, \quad 79, \quad 83, \quad 87, \quad 89, \quad 91, \quad 93, \quad 97$$

11.24 Seja $a = 8316$ e $b = 10\,920$.

(*a*) Ache $d = \text{mdc}(a, b)$, o máximo divisor comum de a e b.

(*b*) Ache inteiros m e n tais que $d = ma + nb$.

(*c*) Ache o mmc (a, b), o mínimo múltiplo comum de a e b.

(*a*) Divida o maior número $b = 10\,920$, pelo menor $a = 8316$; então, repetidamente divida cada divisor pelo resto, até obter resto zero. Esses passos estão representados na Figura 11.7. O último resto não nulo é 84. Logo,

$$84 = \text{gcd}\,(8316,\ 10\,920)$$

$$\begin{array}{r|l} 10920 & 8316 \\ -\,8316 & 1 \\ \hline 2604 & \end{array} \qquad \begin{array}{r|l} 8316 & 2604 \\ -\,7812 & 3 \\ \hline 504 & \end{array} \qquad \begin{array}{r|l} 2604 & 504 \\ -\,2520 & 5 \\ \hline 84 & \end{array} \qquad \begin{array}{r|l} 504 & 84 \\ -\,504 & 6 \\ \hline 0 & \end{array}$$

Fig. 11-7

(*b*) Agora, determinamos m e n tais que

$$84 = 8316m + 1092n$$

Dos primeiros três quocientes da Figura 11-7, obtemos as equações:

(*1*) $10\,920 = 1(8316) + 2604$; ou $2604 = 10\,920 - 1(8316)$

(*2*) $8316 = 3(2604) + 504$; ou $504 = 8316 - 3(2604)$

(*3*) $2604 = 5(504) + 84$; ou $84 = 2604 - 5(504)$

A equação (*3*) nos diz que 84 é uma combinação linear de 2604 e 504. Usamos (*2*) para substituir 504 em (*3*), de tal forma que podemos escrever 84 como combinação linear de 2604 e 8316 como a seguir

(*4*) $84 = 2604 - 5(8316 - 3(2604)) = 2604 - 5(8316) + 15(2604)$
$= 16(2604) - 5(8316)$

Agora usamos (*1*) para substituir 2604 em (*4*) de tal maneira que 84 pode ser escrito como uma combinação linear de 8316 e 10 920 como a seguir:

$$\begin{aligned} 84 &= 16(10\,920 - 1(8316)) - 5(8316) \\ &= 16(10\,920) - 16(8316) - 5(8316) \\ &= -21(8316) + 16(10\,920) \end{aligned}$$

Esta é a combinação linear pedida. Logo, $m = -21$ e $n = 16$.

(*c*) Pelo Teorema 11.15,

$$\text{mmc}\,(a, b) = \frac{|ab|}{\text{mdc}\,(a, b)} = \frac{(8316)(10\,920)}{84} = 1\,081\,080$$

11.25 Seja $a = 37$ e $b = 249$. (*a*) Ache $d = \text{mdc}(a, b)$. (*b*) Ache inteiros m e n tais que $d = ma + nb$. (*c*) Ache mmc (a, b).

(*a*) Divida o maior número $b = 249$ pelo menor $a = 37$, e então, repetidamente divida cada divisor pelo resto até obter resto igual a zero. Esses passos estão representados na Figura 11-8. O último resto não nulo é 1. Logo,

$$\begin{array}{r|l} 249 & 37 \\ -\,222 & 6 \\ \hline 27 & \end{array} \qquad \begin{array}{r|l} 37 & 27 \\ -\,27 & 1 \\ \hline 10 & \end{array} \qquad \begin{array}{r|l} 27 & 10 \\ -\,20 & 2 \\ \hline 7 & \end{array} \qquad \begin{array}{r|l} 10 & 7 \\ -\,7 & 1 \\ \hline 3 & \end{array} \qquad \begin{array}{r|l} 7 & 3 \\ -\,6 & 2 \\ \hline 1 & \end{array} \qquad \begin{array}{r|l} 3 & 1 \\ -\,3 & 3 \\ \hline 0 & \end{array}$$

Fig. 11-8

Hidden page

11.28 Prove o Teorema 11.8: suponha que a, b e c são inteiros.

(i) Se $a|b$ e $b|c$, então $a|c$.

(ii) Se $a|b$, então para qualquer inteiro x, $a|bx$.

(iii) Se $a|b$ e $a|c$, então, $a|(b+c)$ e $a|(b-c)$.

(iv) Se $a|b$ e $b \neq 0$, então $a = \pm b$ ou $|a| < |b|$.

(v) Se $a|b$ e $b|a$, então $|a| = |b|$, i.e., $a = \pm b$.

(vi) Se $a|1$, então $a = \pm 1$.

(i) Se $a|b$ e $b|c$, então existem inteiros x e y tais que $ax = b$ e $by = c$. Substituindo b por ax, obtemos $axy = c$. Logo, $a|c$.

(ii) Se $a|b$, então existe um inteiro c tal que $ac = b$. Multiplicando a equação por x, obtemos $acx = bx$. Logo, $a|bx$.

(iii) Se $a|b$ e $a|c$, existem inteiros x e y tais que $ax = b$ e $ay = c$. Somando as igualdades, obtemos

$$ax + ay = b + c \qquad \text{e, portanto,} \qquad a(x+y) = b + c$$

Logo, $a|(b+c)$. Subtraindo as igualdades, obtemos

$$ax - ay = b - c \qquad \text{e, portanto,} \qquad a(x-y) = b - c.$$

Logo, $a|(b-c)$.

(iv) Se $a|b$, existe c tal que $ac = b$. Então,

$$|b| = |ac| = |a|\ |c|$$

Pelo Problema 11.12(b), ou $|c| = 1$ ou $|a| < |a|\ |c| = |b|$. Se $|c| = 1$, então $c = \pm 1$, de onde segue que $a = \pm b$, como queríamos mostrar.

(v) Se $a|b$, então $a = \pm b$ ou $|a| < |b|$. Se $|a| < |b|$, $b \nmid a$. Logo, $a = \pm b$.

(vi) Se $a|1$, então $a = \pm 1$ ou $|a| < |1| = 1$. Pelo Problema 11.2(a), $|a| \geq 1$. Logo, $a = \pm 1$.

11.29 Um subconjunto não vazio J de $\mathbf{Z}$ é dito um *ideal* se J tem as seguintes propriedades:

(1) Se $a, b \in J$, então $a + b \in J$.

(2) Se $a \in J$ e $n \in \mathbf{Z}$, então $na \in J$.

Seja d o menor inteiro positivo em um ideal $J \neq \{0\}$. Prove que d divide qualquer elemento de J.

Como $J \neq \{0\}$, existe $a \in J$ com $a \neq 0$. Portanto, $-a = -1(a) \in J$. Logo, J contém elementos positivos. Pelo princípio da boa ordenação, J contém um menor elemento positivo e, logo, d existe. Agora, considere $b \in J$. Dividindo b por d, o algoritmo de divisão nos diz que existem d e q tais que

$$b = qd + r \qquad \text{e} \qquad 0 \leq r < d$$

Porém, b e $d \in J$, e J é um ideal; portanto, $b + (-q)d = r$ também pertence a J. Pela minimalidade de d, precisamos ter $r = 0$. Logo, $d|b$, como queríamos provar.

11.30 Prove o Teorema 11.12: seja d o menor inteiro positivo da forma $ax + by$. Então, $d = \text{mdc}(a, b)$.

Considere o conjunto $J = \{ ax + by : x, y \in \mathbf{Z}\}$. Então,

$$a = 1(a) + 0(b) \in J \quad \text{e} \quad b = 0(a) + 1(b) \in J$$

Suponha também que s e $t \in J$, digamos, $s = x_1a + y_1b$ e $t = x_2a + y_2b$. Então, para qualquer $n \in \mathbf{Z}$,

$$s + t = (x_1 + x_2)a + (y_1 + y_2)b \qquad \text{e} \qquad ns = (nx_1)a + (ny_1)b$$

também pertencem a J. Portanto, J é um ideal. Seja d o menor elemento positivo em J. Afirmamos que $d = \text{mdc}(a, b)$.

Pelo Problema 11.28, d divide qualquer elemento de J. Logo, em particular, d divide a e b. Suponha agora que h divide ambos, a e b. Então, h divide $xa + yb$ para todo x e y; isto é, h divide todo elemento de J. Portanto, h divide d e, portanto, $h \leq d$. Conseqüentemente, $d = \text{mdc}(a, b)$.

11.31 Prove o Teorema 11.16: suponha que $\text{mdc}(a, b) = 1$, e a e b dividem c. Então ab divide c.

Como $\text{mdc}(a, b) = 1$, existem x e y tais que $ax + by = 1$. Como $a|c$ e $b|c$, existem m e n tais que $c = ma$ e $c = nb$. Multiplicando $ax + by = 1$ por c, obtém-se

$$acx + bcy = c \qquad \text{ou} \qquad a(nb)x + b(ma)y = c \qquad \text{ou} \qquad ab(nx + my) = c$$

Logo, ab divide c.

11.32 Prove o Corolário 11.18: suponha que um primo p divide o produto ab. Então, $p|a$ ou $p|b$.

Suponha que p não divida a. Então, $\text{mdc}(p, a) = 1$ já que os únicos divisores de p são ± 1 e $\pm p$. Portanto, existem inteiros m e n tais que $1 = mp + na$. Multiplicando por b, obtém-se $b = mbp + nab$. Por hipótese, p divide ab, isto é, $ab = cp$. Então,

$$b = mpb + nab = mpb + ncp = p(mb + nc).$$

Logo, $p|b$, como queríamos provar.

11.33 Prove: (*a*) suponha que $p|q$ e que p e q são primos. Então, $p = q$. (*b*) Suponha $p|q_1 q_2 \cdots q_r$ onde p e q são primos. Então, p é igual a algum dos qs.

(*a*) Os únicos divisores de q são ± 1 e $\pm q$. Como $p > 1$, $p = q$.

(*b*) Se $r = 1$, então $p = q_1$ por (*a*). Suponha que $r > 1$. Pelo Problema 11.32 (Corolário 11.18), $p|q_1$ ou $p|(q_2 \cdots q_r)$. Se $p|q_1$, então $p = q_1$ por (*a*). Senão, então $p|(q_2 \cdots q_r)$. Repetimos o argumento. Isto é, obtemos $p = q_2$ ou $p|(q_3 \cdots q_r)$. Finalmente (ou por indução), p deve ser igual a algum dos qs.

11.34 Prove o teorema fundamental da aritmética (Teorema 11.19): todo inteiro $n > 1$ pode ser expresso de maneira única (exceto pela ordem) como um produto de primos.

Já provamos o Teorema 11.10 que diz que um tal produto de primos existe. Portanto, precisamos mostrar apenas que o produto é único (exceto pela ordem). Suponha que

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$$

onde os ps e qs são primos. Note que $p_1|(q_1 \cdots q_r)$. Pelo Problema 11.33, p_1 é igual a algum dos qs. Reordenamos os qs de tal modo que $p_1 = q_1$. Então,

$$p_1 p_2 \cdots p_k = p_1 q_2 \cdots q_r \qquad \text{e, portanto,} \qquad p_2 \cdots p_k = q_2 \cdots q_r$$

Pelo mesmo argumento, podemos reordenar os qs remanescentes de modo a ter $p_2 = q_2$. E assim por diante. Logo, n pode ser expresso de maneira única como um produto de primos (exceto pela ordem).

Congruências

11.35 Quais das seguintes congruências é verdadeira?

(*a*) $446 \equiv 278 \pmod 7$. (*d*) $473 \equiv 369 \pmod{26}$.

(*b*) $793 \equiv 682 \pmod 9$. (*e*) $445 \equiv 536 \pmod{18}$.

(*c*) $269 \equiv 413 \pmod{12}$. (*f*) $383 \equiv 126 \pmod{15}$.

Lembre que $a \equiv b \pmod m$ se e somente se m divide $a - b$.

(*a*) **Método 1:** Ache a diferença $446 - 278 = 168$. Divida a diferença 168 pelo *modulus* $m = 7$. O resto é 0; logo, a afirmação é verdadeira.

Método 2: Reduza cada um dos lados módulo 7. Dividindo 446 por 7, obtemos resto $r = 5$, e dividindo 278 por 7, também obtemos resto $r = 5$. Logo, $446 \equiv 278 \pmod 7$.

(*b*) Divida a diferença $793 - 682 = 111$ pelo *modulus* $m = 9$. O resto não é zero. Logo, a afirmativa é falsa. (Como segunda opção, dividindo 793 por 9, obtém-se resto $r = 1$, mas dividindo 682 por 9, obtém-se resto $r = 6$.)

(*c*) Verdadeira, já que 12 divide $269 - 413 = -144$.

(*d*) Verdadeira, já que 26 divide $472 - 359 = 104$.

(*e*) Falsa, já que 18 não divide $445 - 536 = -91$.

(*f*) Falsa, já que 15 não divide $383 - 126 = 157$.

11.36 Ache o menor inteiro não negativo que é congruente módulo $m = 8$ a cada um dos seguintes números: (*a*) 379; (*b*) 695; (*c*) – 578; (*d*) –285.

[O inteiro deve estar no conjunto {0, 1, 2,..., 7}.]

(*a*) Dividindo 379 por $m = 8$, obtemos resto 3; logo,

$$379 \equiv 3 \pmod 8$$

(*b*) Dividindo 695 por $m = 8$, obtemos resto 7; logo,

$$695 \equiv 7 \pmod 8$$

(*c*) Dividindo 578 por $m = 8$, obtemos resto 2; logo,

$$-578 \equiv -2 \equiv 6 \pmod 8$$

(Obtemos 6 pela adição do módulo $m = 8$ com –2.)

(*d*) Dividindo 285 por $m = 8$, obtemos resto 5; logo,

$$-285 \equiv -5 \equiv 3 \pmod 8$$

11.37 Ache o menor inteiro em valor absoluto que é congruente módulo $m = 7$ a cada um dos seguintes números:

(*a*) 386; (*b*) 257; (*c*) –192; (*d*) –466.

[O inteiro deve estar no conjunto {–3, –2, –1, 0, 1, 2, 3}.]

(*a*) Dividindo 386 por $m = 7$ obtemos resto 1; logo,

$$386 = 1 \pmod 7$$

(*b*) Dividindo 257 por $m = 7$, obtemos resto 5; logo,

$$257 \equiv 5 \equiv -2 \pmod 7$$

(Obtemos –2 subtraindo o *modulus* $m = 7$ de 5)

(*c*) Dividindo 192 por $m = 7$ obtemos resto 3; logo,

$$-192 \equiv -3 \pmod 7$$

(*d*) Dividindo 466 por $m = 8$ obtemos resto 4; logo,

$$-466 \equiv -4 \equiv 3 \pmod 7$$

(Obtemos 3 subtraindo o *modulus* $m = 7$ a – 4.)

11.38 Ache os números entre 1 e 100 que são congruentes a 6 módulo $m = 13$, isto é, ache todos os valores de x tais que $1 \le x \le 100$ e

$$x \equiv 6 \pmod{13}$$

Some múltiplos do módulo $m = 13$ ao número dado 6 para obter

$$6 + 0 = 6, \quad 6 + 13 = 19, \quad 19 + 13 = 32, \quad 32 + 13 = 45$$
$$45 + 13 = 58, \quad 58 + 13 = 71, \quad 71 + 13 = 84, \quad 84 + 13 = 97$$

Isto é,

$$6, \quad 19, \quad 32, \quad 45, \quad 58, \quad 71, \quad 84, \quad 97$$

11.39 Ache todos os números entre –50 e 50 que são congruentes a 21 módulo $m = 12$. Isto é, ache todos os x tais que $-50 \le x \le 50$ e

$$x \equiv 21 \pmod{12}$$

Some e subtraia múltiplos do módulo $m = 12$ ao número dado 21 para obter

$$21 + 0 = 21, \quad 21 + 12 = 33, \quad 33 + 12 = 46, \quad 21 - 12 = 9$$
$$9 - 12 = -3, \quad -3 - 12 = -15, \quad -15 - 12 = -27, \quad -27 - 12 = -39$$

Isto é,

$$-39, \quad -27, \quad -15, \quad -3, \quad 9, \quad 21, \quad 33, \quad 46$$

11.40 Prove o Teorema 11.20: seja m um inteiro positivo. Então:

(i) Para todo inteiro a, temos $a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(iv) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

(i) A diferença $a - a = 0$ é divisível por m; logo, $a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, então $m|(a - b)$. Logo, m divide $-(a - b) = b - a$. Logo, $b \equiv a \pmod{m}$.

(iii) Sabemos que $m|(a - b)$ e $m|(b - c)$. Logo, m divide a soma $(a - b) + (b - c) = a - c$. Logo, $a \equiv c \pmod{m}$.

11.41 Prove o Teorema 11.21: suponha que $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$. Então:

(i) $a + b \equiv c + d \pmod{m}$.

(ii) $a \cdot b \equiv c \cdot d \pmod{m}$

Sabemos que $m|(a - c)$ e $m|(b - d)$.

(i) Então, m divide a soma $(a - c) + (b - d) = (a + b) - (c + d)$. Logo,

$$a + b \equiv c + d \pmod{m}$$

(ii) Então, m divide o produto $b(a - c) = ab - bc$, e m divide o produto $c(b - d) = bc - cd$. Logo, m divide a soma

$$(ab - bc) + (bc - cd) = ab - cd$$

Portanto, $ab \equiv cd \pmod{m}$

11.42 Prove: se $a + b \equiv a + c \pmod{m}$, então $b \equiv c \pmod{m}$.

(Isto é, a lei do cancelamento vale para a adição módulo m.)

Por hipótese, m divide a diferença $(a + b) - (a + c) = b - c$. Logo, $b \equiv c \pmod{m}$, como queríamos provar.

11.43 Seja $d = \text{mdc}(a, b)$. Mostre que a/b e b/d são relativamente primos.

Existem x e y tais que $d = xa + yb$. Dividindo a equação por d, obtemos $1 = x(a/d) + y(b/d)$. Logo, a/b e b/d são relativamente primos.

11.44 Prove o Teorema 11.23: suponha que $ab \equiv ac \pmod{m}$ e $d = \text{mdc}(a, m)$. Então, $b \equiv c \pmod{m/d}$.

Por hipótese, m divide $ab - ac = a(b - c)$. Logo, existe um inteiro x tal que $a(b - c) = mx$. Dividindo por d, obtém-se

$$(a/d)(b - c) = (m/d)x$$

Logo, m/d divide $(a/d)(b - c)$. Como m/d e a/d são relativamente primos, m/d divide $b - c$. Isto é, $b \equiv c \pmod{m/d}$, como queríamos provar.

Sistemas de Resíduos, Função Phi (ϕ) de Euler

11.45 Para cada módulo m, exiba dois sistemas completos de resíduos; um com os menores inteiros não negativos e outro com os inteiros de menor valor absoluto.

$$(a)\ m = 9; \quad (b)\ m = 12.$$

No primeiro caso, escolha $\{0, 1, 2, \ldots, m - 1\}$ e, no segundo caso, escolha

$$\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\} \quad \text{ou} \quad \{-(m-2)/2, \ldots, -1, 0, 1, \ldots, m/2\}$$

dependendo de m ser ímpar ou par:

(*a*) $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ e $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.

(*b*) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ e $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$.

11.46 Exiba um sistema reduzido de resíduos módulo m e ache $\phi(m)$ onde: (*a*) $m = 9$; (*b*) $m = 12$; (*c*) $m = 13$; (*d*) $m = 16$.

Escolha os números positivos menores do que m e os primos relativos de m. A cardinalidade do conjunto obtido é $\phi(m)$.

(*a*) $\{1, 2, 4, 5, 7, 8\}$; portanto, $\phi(9) = 6$.

(*b*) $\{1, 5, 7, 11\}$; portanto, $\phi(12) = 4$.

(*c*) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$; portanto, $\phi(13) = 12$. [Isso era esperado, pois $\phi(p) = p - 1$ para qualquer primo p.]

(*d*) $\{1, 3, 5, 7, 9, 11, 13, 15\}$; portanto, $\phi(16) = 8$.

11.47 Lembre que $S_m = \{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Prove:

(*a*) Quaisquer m inteiros consecutivos formam um sistema completo de resíduos módulo m.

(*b*) Se $\text{mdc}(a, m) = 1$, então $aS_m = \{0, a, 2a, 3a, \ldots, (m-1)a\}$ é um sistema completo de resíduos módulo m.

(*a*) Considere qualquer outra seqüência de inteiros, por exemplo,

$$\{a, a+1, a+2, \ldots, a+(m-1)\}$$

O valor absoluto da diferença s de quaisquer dois dos inteiros é menor do que m. Logo, m não divide s e, portanto, os números não são congruentes módulo m.

(*b*) Suponha que $ax \equiv ay \pmod{m}$ onde x e $y \in S_m$. Como $\text{mdc}(a, m) = 1$, a lei do cancelamento modificada, Teorema 11.23, nos diz que $x \equiv y \pmod{m}$. Como x e $y \in S_m$, precisamos ter $x = y$. Isto é, S_m é um sistema completo de resíduos módulo m.

11.48 Exiba um sistema completo de resíduos módulo $m = 8$ formado inteiramente por múltiplos de 3.

Pelo Problema 11.47(*b*), $3S_8 = \{0, 3, 6, 9, 12, 15, 18, 21\}$ é um sistema completo de resíduos módulo $m = 8$.

11.49 Mostre que, se p é um primo, então

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

Claramente, $\text{mdc}(a, p^n) \neq 1$ se e somente se p divide a. Logo, os únicos números entre 1 e p^n que não são primos relativos com p^n são os múltiplos de p, isto é,

$$p, \quad 2p, \quad 3p, \quad \ldots, \quad p^{n-1}(p)$$

Existem p^{n-1} de tais múltiplos de p. Todos os outros números entre 1 e p^n são primos relativos com p^n. Logo,

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

como afirmamos.

11.50 Ache (*a*) $\phi(81), \phi(125), \phi(7^6)$; (*b*) $\phi(72), \phi(3000)$.

(*a*) Pelo Problema 11.49,

$$\phi(81) = \phi(3^4) = 3^3(2-1) = 27(2) = 54$$
$$\phi(125) = \phi(5^3) = 5^2(5-1) = 25(4) = 100$$
$$\phi(7^6) = 7^5(7-1) = 6(7^5)$$

(*b*) Use o Teorema 11.24 que diz que ϕ é multiplicativo

$$\phi(72) = \phi(3^2 \cdot 2^3) = \phi(3^2)\phi(2^3) = 3(3-1) \cdot 2^2(2-1) = 24$$
$$\phi(3000) = \phi(3 \cdot 2^2 \cdot 5^3) = \phi(3)\phi(2^2)\phi(5^3) = 2 \cdot 2 \cdot 5^2(5-1) = 400$$

Hidden page

11.53 Em $\mathbf{Z}_{11}$, ache (*a*) $-2, -3, -5, -8, -9, -10$; (*b*) $2/7, 3/7, 5/7, 8/7, 10/7, 1/7$.

(*a*) Note que $-a = m - a$, pois $(m - a) + a = 0$. Logo,

$$-2 = 11 - 2 = 9, \qquad -5 = 11 - 5 = 6, \qquad -9 = 11 - 9 = 2$$
$$-3 = 11 - 3 = 8, \qquad -8 = 11 - 8 = 3, \qquad -10 = 11 - 10 = 1$$

(*b*) Por definição, a/b é o inteiro c tal que $bc = a$. Como estamos dividindo por 7, primeiramente escreva a tabela de multiplicação por 7 em $\mathbf{Z}_{11}$, isto é,

×	0	1	2	3	4	5	6	7	8	9	10
7	0	7	3	10	6	2	9	5	1	8	4

Agora localize na tabela o número, e a resposta estará acima do número. Logo,

$$2/7 = 5, \qquad 3/7 = 2, \qquad 5/7 = 7, \qquad 8/7 = 9, \qquad 10/7 = 3, \qquad 1/7 = 8$$

[Note que $7^{-1} = 8$, já que $7(8) = 8(7) = 1$.]

11.54 Considere $\mathbf{Z}_p$ onde p é um primo. Prove:

(*a*) Se $ab = ac$ e $a \neq 0$, então $b = c$.

(*b*) Se $ab = 0$, então $a = 0$ ou $b = 0$.

(*a*) Se $ab = ac$ em $\mathbf{Z}_p$, então $ab \equiv ac \pmod{p}$. Como $a \neq 0$, $\text{mdc}(a, p) = 1$. Pelo Teorema 11.22, podemos cancelar os a para obter

$$b \equiv c \pmod{p}$$

Logo, $b = c$ em $\mathbf{Z}_p$.

(*b*) Se $ab = 0$ em $\mathbf{Z}_p$, então $ab \equiv 0 \pmod{p}$. Portanto, p divide o produto ab. Como p é primo, $p|a$ ou $p|b$; isto é,

$$a \equiv 0 \pmod{p} \qquad \text{ou} \qquad b \equiv 0 \pmod{p}$$

Logo, $a = 0$ ou $b = 0$ em $\mathbf{Z}_p$.

11.55 Considere $a \neq 0$ em $\mathbf{Z}_m$ onde $\text{mdc}(a, m) = 1$. Mostre que a tem um inverso multiplicativo em $\mathbf{Z}_m$.

Como $a \neq 0$ e $\text{mdc}(a, m) = 1$, existem inteiros x e y tais que $ax + my = 1$ ou $ax - 1 = my$. Portanto, m divide $ax - 1$e, logo, $ax \equiv 1 \pmod{m}$. Escreva x módulo m como um elemento x' em $\mathbf{Z}_m$. Então, $ax' = 1$ em $\mathbf{Z}_m$.

11.56 Ache a^{-1} em $\mathbf{Z}_m$ onde (*a*) $a = 37$ e $m = 249$; (*b*) $a = 15$ e $m = 234$.

(*a*) Ache $d = \text{mdc}(37, 249)$, como no Problema 11.25. Como $d = \text{mdc}(37, 249) = 1$, a^{-1} existe. Ache os inteiros x e y tais que $37x + 249y = 1$. Pelo Problema 11.25,

$$-74(37) + 11(249) = 1 \qquad \text{e assim} \qquad -74(37) \equiv 1 \pmod{249}$$

Some $m = 249$ a -74 para obter $-74 + 249 = 175$. Logo,

$$(175)(37) \equiv 1 \pmod{249}$$

Portanto, $a^{-1} = 175$ em $\mathbf{Z}_{249}$.

(*b*) Ache $d = \text{mdc}(15, 234) = 3$. Logo, $d \neq 1$ e, portanto, 15 não tem inverso multiplicativo em $\mathbf{Z}_{234}$.

11.57 Considere os seguintes polinômios sobre $\mathbf{Z}_7$:

$$f(x) = 6x^3 - 5x^2 + 2x - 4, \qquad g(x) = 5x^3 + 2x^2 + 6x - 1, \qquad h(x) = 3x^2 - 2x - 5$$

Ache: (*a*) $f(x) + g(x)$; (*b*) $f(x)\,h(x)$.

Faça as operações como se os polinômios fossem definidos sobre os inteiros $\mathbf{Z}$, e então reduza o coeficientes módulo 7.

(*a*) Temos

$$\begin{array}{r} 6x^3 - 5x^2 + 2x - 4 \\ \hline 5x^3 + 2x^2 + 6x - 4 \\ \hline 11x^3 - 3x^2 + 8x - 5 \end{array} \quad \text{ou} \quad 4x^3 - 3x^2 + x - 5 \quad \text{ou} \quad 4x^3 + 4x^2 + x + 2$$

(*b*) Temos

$$\begin{array}{r} 6x^3 - 5x^2 + 2x - 4 \\ 3x^2 - 2x \ - 5 \\ \hline 18x^5 - 15x^4 + \ 6x^3 - 12x^2 \\ \quad - 12x^4 + 10x^3 - \ 4x^2 + \ 8x \\ \hline \quad - 30x^2 + 25x^2 - 10x + 20 \\ \hline 18x^5 - 27x^4 + 14x^3 + 9x^2 \ - \ 2x + 20 \end{array}$$

ou $4x^5 - 6x^4 + 2x^2 - 2x + 6$

ou $4x^5 + x^4 + 2x^2 + 5x + 6$

Equações de Congruência

11.58 Resolva a equação de congruência $f(x) = 4x^4 - 3x^3 + 2x^2 + 5x - 4 \equiv 0 \pmod 6$.

Como a equação não é linear, resolvemos a equação testando os números em um sistema completo de resíduos módulo 6. Digamos,

$$\{0, 1, 2, 3, 4, 5\}$$

Temos

$$\begin{aligned} f(0) &= -4 \not\equiv 0 \pmod 6 \\ f(1) &= 4 - 3 + 2 + 5 - 4 = 4 \not\equiv 0 \pmod 6 \\ f(2) &= 64 - 24 + 8 + 10 - 4 = 54 \equiv 0 \pmod 6 \\ f(3) &= 324 - 81 + 18 + 15 - 4 = 272 \equiv 2 \not\equiv 0 \pmod 6 \\ f(4) &= 1024 - 192 + 32 + 20 - 4 = 880 \equiv 4 \not\equiv 0 \pmod 6 \\ f(5) &= 2500 - 375 + 50 + 25 - 4 = 2196 \equiv 0 \pmod 6 \end{aligned}$$

Portanto, apenas 2 e 5 são raízes de $f(x)$ módulo 6. Isto é, $\{2, 5\}$ é um conjunto completo de soluções.

11.59 Resolva a equação de congruência

$$f(x) = 26x^4 - 31x^3 + 46x^2 - 76x + 57 \equiv 0 \pmod 8$$

Primeiramente reduza os coeficientes de $f(x)$ módulo 8 para obter a equação de congruência equivalente

$$g(x) = 2x^4 - 7x^3 + 6x^2 - 4x + 1 \equiv 0 \pmod 8$$

Como $7 \equiv -1 \pmod 8$ e $6 \equiv -2 \pmod 8$, podemos simplificar a equação original para obter a equação de congruência equivalente

$$h(x) = 2x^4 + x^3 - 2x^2 - 4x + 1 \equiv 0 \pmod 8$$

Testamos os números em um sistema completo de resíduos módulo 8 e, para manter nossa aritmética o mais simples possível, escolhemos

$$\{-3, -2, -1, 0, 1, 2, 3, 4\}$$

(Isto é, escolhemos os números cujos valores absolutos são mínimos.) Substituindo esses números em $h(x)$, obtemos:

$$\begin{aligned} h(-3) &= 130 \equiv 2 \pmod 8, & h(1) &= -2 \equiv 6 \pmod 8 \\ h(-2) &= 25 \equiv 1 \pmod 8, & h(2) &= 25 \equiv 1 \pmod 8 \\ h(-1) &= 94 \equiv 4 \pmod 8, & h(3) &= 160 \equiv 0 \pmod 8 \\ h(0) &= 91 \equiv 1 \pmod 8, & h(4) &= 513 \equiv 1 \pmod 8 \end{aligned}$$

Portanto, 3 é a única solução de $f(x) \pmod 8$.

11.60 Resolva cada equação linear de congruência:
(*a*) $3x \equiv 2 \pmod 8$; (*b*) $6x \equiv 5 \pmod 9$; (*c*) $4x \equiv 6 \pmod{10}$

Como os *moduli* são relativamente pequenos, achamos todas as soluções por inspeção. Lembre que $ax \equiv b \pmod m$ tem exatamente $d = \text{mdc}(a, m)$ soluções quando d divide b.

(*a*) Aqui, mdc(3, 8) = 1. Logo, a equação tem uma única solução. Testando 0, 1, 2, ...,7, verificamos que

$$3(6) = 18 \equiv 2 \pmod 8$$

(*b*) Aqui, mdc(6, 9) = 3, mas 3 não divide 5. Logo, o sistema não tem solução.

(*c*) Aqui, mdc(4, 10) = 2, e 2 divide 6; portanto, o sistema tem duas soluções.

Método 1: Testando 0, 1, 2, 3,..., 9, vemos que

$$4(4) = 16 \equiv 6 \pmod{10} \qquad \text{e} \qquad 4(9) = 36 \equiv 6 \pmod{10}$$

Portanto, 4 e 9 são as duas soluções.

Método 2: Divida a equação e o *modulus* por mdc(4, 10) = 2 para obter a equação de congruência:

$$2x \equiv 3 \pmod 5$$

A única solução dessa equação é $x = 4$, que é solução da equação original. Some o novo *modulus* 5 a esta solução para obter

$$x = 4 + 5 = 9$$

Que é a segunda solução da equação original. Portanto, 4 e 9 são as duas soluções desejadas.

11.61 Resolva a equação de congruência $1092x \equiv 23 \pmod{2295}$

Não é eficiente resolver esta equação por testes diretos, já que o *modulus* $m = 2295$ é muito grande. Primeiramente, use o algoritmo de divisão para achar $d = \text{mdc}(1092, 2295) = 3$. Dividindo 21 por $d = 3$, obtém-se 0 como resto; isto é, 3 divide 213. Logo, a equação terá três soluções não congruentes.

Divida a equação e o *modulus* $m = 2295$ por $d = 3$ para obter a equação de congruência

$$364x \equiv 71 \pmod{765} \qquad (*)$$

Sabemos que 364 e 765 são primos relativos, já que foram obtidos da divisão por $d = \text{mdc}(1092, 2295) = 3$; logo a equação $(*)$ tem uma única solução módulo 765. Resolvemos $(*)$ determinando primeiramente a solução da equação

$$364x \equiv 1 \pmod{765} \qquad (**)$$

Essa solução é obtida determinando s e t tais que

$$364s + 765t = 1$$

Isto pode ser feito usando o algoritmo de divisão (como no Problema 11.25).

$$\begin{array}{r|l} 765 & 2 \\ -728 & 364 \\ \hline 37 & \end{array} \qquad \begin{array}{r|l} 364 & 37 \\ -333 & 3 \\ \hline 31 & \end{array} \qquad \begin{array}{r|l} 37 & 31 \\ -31 & 1 \\ \hline 6 & \end{array} \qquad \begin{array}{r|l} 31 & 6 \\ -30 & 5 \\ \hline 1 & \end{array}$$

Fig. 11-22

Especificamente, divida $m = 765$ por $a = 364$ e, repetidamente, divida cada divisor pelo resto como na Figura 11-12. Os quocientes na Figura 11-12 geram as seguintes quatro equações:

(*1*) $37 = 765 - 2(364)$
(*2*) $31 = 364 - 9(37)$
(*3*) $6 = 37 - 1(31)$
(*4*) $1 = 31 - 5(6)$

Usando (*4*) e (*3*), escreva 1 como combinação linear de 31 e 37 como a seguir:

(*5*) $1 = 31 - 5[37 - 1(31)] = 6(31) - 5(37)$

Usando (*5*) e (*2*), escreva 1 como combinação linear de 364 e 37 como a seguir:

(*6*) $1 = 6[364 - 9(37)] - 5(37) = 6(364) - 59(37)$

Usando (*6*) e (*1*), escreva 1 como combinação linear de 364 e 765 como a seguir:

(*7*) $1 = 6(364) - 59[765 - 2(364)] = 124(364) - 59(765)$

Logo, $s = 124$ e $t = -59$.

Conseqüentemente, $s = 124$ é a única solução de $(**)$. Multiplicando esta solução $s = 124$ por 71 e reduzindo módulo 765, obtemos

$$124(71) = 8804 \equiv 389 \pmod{765}$$

Essa é a única solução de $(*)$.

Finalmente, somamos o novo módulo $m = 765$ à solução $x_1 = 389$ duas vezes para obter as outras duas soluções da equação dada:

$$x_2 = 389 + 765 = 1154, \qquad x_3 = 1154 + 765 = 1919$$

Em outras palavras, $x_1 = 389$, $x_2 = 1154$ e $x_3 = 1919$ formam um conjunto completo de soluções da equação dada $1092x \equiv 213 \pmod{2295}$.

11.62 Resolva a equação de congruência $455x \equiv 204 \pmod{469}$.

Primeiramente use o algoritmo de divisão para achar $d = \text{mdc}(455, 469) = 7$. Dividindo 204 por $d = 7$, obtemos 1 como resto; isto é, 7 não divide 204. Logo, a equação não tem solução.

11.63 Um menino vende maçãs por 12 centavos cada, e peras por 7 centavos cada. Suponha que o garoto tenha ganho $3,21. Quantas maçãs e peras ele vendeu?

Sejam x e y, respectivamente, o número de maçãs e peras vendidas. Obtemos assim a equação diofantina

$$12x + 7y = 321 \qquad (*)$$

(Essa é uma *equação diofantina*, pois x e y estão restritos aos inteiros positivos.) A equação $(*)$ é equivalente à equação de congruência

$$12x \equiv 321 \pmod{7}$$

Reduzindo a equação módulo 7, obtemos a equação equivalente

$$5x \equiv 6 \pmod{7}$$

Testando 0, 1,..., 6, obtemos a única solução

$$x = 4$$

Somamos os múltiplos do módulo $m = 7$ a 4 para obter os valores possíveis de x e, em cada caso, substituímos em $(*)$ para calcular o valor correspondente de y. Obtemos

$$x = 4,\ y = 39; \qquad x = 11,\ y = 27; \qquad x = 18,\ y = 15$$

Como $12(25) = 400$ é maior do que 321, $x = 25$, e qualquer valor maior para x produzirá um valor negativo para y. Conseqüentemente, existem três soluções possíveis:

4 maçãs, 39 peras; 11 maçãs, 27 peras, 18 maçãs, 15 peras

Em outras palavras,

$$x = 4 + 7t \qquad \text{e} \qquad y = 39 - 12t$$

é a solução geral de $(*)$, e $t = 0, 1, 2$ são os únicos valores de t que produzem valores não negativos para ambos, x e y.

11.64 Ache o menor inteiro positivo x tal que, se x é dividido por 3, obtém-se resto 2, e quando x é dividido por 7, obtém-se resto 4; e quando x é dividido por 10, obtém-se resto 6.

Procuramos a menor solução positiva comum às três equações

$$(a) \quad x \equiv 2 \pmod 3; \qquad (b) \quad x \equiv 4 \pmod 7; \qquad (c) \quad x \equiv 6 \pmod{10}$$

Observe que os *moduli* 3, 7 e 10 são, dois a dois, relativamente primos. (*Moduli* é plural de *modulus*.) O teorema do resto chinês (TRC) 11.28 nos diz que existe uma única solução módulo do produto $m = 3(7)(10) = 210$. Resolvemos o problema de duas maneiras.

Metodo 1: Primeiramente aplique o TRC para as duas equações:

$$(a) \quad x \equiv 2 \pmod 3 \qquad \text{e} \qquad (b) \quad x \equiv 4 \pmod 7$$

Sabemos que existe uma única solução módulo $M = 3 \cdot 7 = 21$. Somando múltiplos de $m = 7$ à solução dada da segunda equação (b) $x = 4$, obtemos as seguintes três soluções de (b) que são menores do que 21:

$$4, \quad 11, \quad 18$$

Testando cada uma das soluções de (b) na equação (a), verificamos que 11 é a única solução das duas equações.

Agora aplicamos o mesmo processo às duas equações

$$(c) \quad x \equiv 6 \pmod{10} \qquad \text{e} \qquad (d) \quad x \equiv 11 \pmod{21}$$

O TRC nos diz que existe uma única solução módulo $M = 21 \cdot 10 = 210$. Somando múltiplos do módulo $m = 21$ à solução dada da equação (d) $x = 11$, obtemos as seguintes 10 soluções de (d) que são menores do que 210:

$$11, \quad 32, \quad 53, \quad 74, \quad 95, \quad 116, \quad 137, \quad 158, \quad 179, \quad 210$$

Testando cada uma das soluções de (d) na equação (c), verificamos que $x = 116$ é a única solução da equação (c). Logo,

$$x = 116$$

é o menor inteiro positivo satisfazendo as três equações dadas (a), (b) e (c).

Método 2: Usando a notação da Proposição 11.29, obtemos

$$M = 3 \cdot 7 \cdot 10 = 210, \qquad M_1 = 210/3 = 70, \qquad M_2 = 210/7 = 30, \qquad M_3 = 210/10 = 21$$

Procuramos soluções para as equações

$$70x \equiv 1 \pmod 3, \qquad 30x \equiv 1 \pmod 7, \qquad 21x \equiv 1 \pmod{10}$$

Reduzindo 70 módulo 3, 30 módulo 7 e 21 módulo 10, obtemos o sistema equivalente

$$x \equiv 1 \pmod 3, \qquad 2x \equiv 1 \pmod 7, \qquad x \equiv 1 \pmod{10}$$

As soluções das três equações são, respectivamente,

$$s_1 = 1, \qquad s_2 = 4, \qquad s_3 = 1$$

Substituindo na fórmula

$$x_0 = M_1 s_1 r_1 + M_2 s_2 r_2 + \cdots + M_k s_k r_k$$

obtemos as seguintes soluções do sistema original:

$$x_0 = 70 \cdot 1 \cdot 2 \quad + \quad 30 \cdot 4 \cdot 4 \quad + \quad 21 \cdot 1 \cdot 6 = 746$$

Dividindo esta solução pelo *modulus* $M = 210$, obtemos o resto

$$x = 116$$

que é a única solução do sistema original entre 0 e 210.

11.65 Prove o Teorema 11.25: se a e m são relativamente primos, então $ax \equiv 1 \pmod{m}$ tem uma única solução; caso contrário, não existe solução.

Suponha que x_0 é uma solução, Então, m divide $ax_0 - 1$ e, portanto, existe y_0 tal que $my_0 = ax_0 - 1$. Portanto,

$$ax_0 + my_0 = 1 \tag{1}$$

e a e m são primos relativos. Conversamente, se a e m são primos relativos, então existe x_0 e y_0 satisfazendo (1) e, neste caso, x_0 é uma solução de $ax \equiv 1 \pmod{m}$.

Resta mostrar que x_0 é a única solução módulo m. Suponha que x_1 é outra solução. Então,

$$ax_0 \equiv 1 \equiv ax_1 \pmod{m}$$

Como a e m são relativamente primos, vale a lei do cancelamento modificada e, logo,

$$x_0 \equiv x_1 \pmod{m}$$

Assim, o teorema está provado.

11.66 Prove o Teorema 11.26: suponha que a e m são primos relativos. Então $ax \equiv b \pmod{m}$ tem uma única solução. Ademais, se s é a única solução de $ax \equiv 1 \pmod{m}$, então $x = bs$ é a única solução de $ax \equiv b \pmod{m}$.

Pelo Teorema 11.25 (provado no Problema 11.65), existe uma solução única s de $ax \equiv 1 \pmod{m}$. Portanto, $as \equiv 1 \pmod{m}$ e, logo,

$$a(bs) = (as)b \equiv 1 \cdot b = b \pmod{m}$$

Isto é, $x = bs$ é uma solução de $ax \equiv b \pmod{m}$. Suponha que x_0 e x_1 são duas soluções. Então,

$$ax_0 \equiv b \equiv ax_1 \pmod{m}$$

Como a e m são primos relativos, a lei do cancelamento modificada nos diz que $x_0 \equiv x_1 \pmod{m}$. Isto é, $ax \equiv b \pmod{m}$ tem uma única solução módulo m.

11.67 Prove o Teorema 11.27: considere a equação

$$ax \equiv b \pmod{m} \tag{*}$$

onde $d = \text{mdc}(a, m)$. (i) Se d não divide b, então a equação $(*)$ não tem solução. (ii) Se d divide b, então a equação $(*)$ tem d soluções, todas elas congruentes módulo M à única solução da equação de

$$Ax \equiv B \pmod{M} \tag{**}$$

onde $A = a/d$, $B = b/d$ e $M = m/d$.

(i) Suponha que x_0 é uma solução de $(*)$. Então, $ax_0 \equiv b \pmod{m}$ e, logo, m divide $ax_0 - b$. Portanto, existe um inteiro y_0 tal que $my_0 = ax_0 - b$ ou $my_0 + ax_0 = b$. Mas $d = \text{mdc}(a, m)$ e, logo, d divide $my_0 + ax_0$. Isto é, d divide b. Conseqüentemente, se d não divide b, não existe solução.

(ii) Suponha que x_0 é uma solução de $(*)$. Então, como acima,

$$my_0 + ax_0 = b$$

Dividindo a equação por d, obtemos $(**)$. Portanto, M divide $Ax_0 - B$ e, logo, x_0 é solução de $(**)$. Conversamente, suponha que x_1 é solução de $(**)$. Então, como acima, existe um inteiro y_1 tal que

$$My_1 + Ax_1 = B$$

Hidden page

Hidden page

Divisibilidade, Máximo Divisor Comum, Primos

11.93 Determine todos os possíveis divisores de (*a*) 24; (*b*) $19\,683 = 3^9$; (*c*) $432 = 2^4 \cdot 3^3$.

11.94 Liste todos os números primos entre 100 e 150.

11.95 Expresse os seguintes números como produto de primos: (*a*) 2940; (*b*) 1485; (*c*) 8712; (*d*) 319 410.

11.96 Para cada par de inteiros a e b, ache $d = \text{mdc}(a, b)$ e expresse d como combinação linear de a e b.

(*a*) $a = 48$, $b = 356$. (*b*) $a = 165$, $b = 1287$. (*c*) $a = 2310$, $b = 168$. (*d*) $a = 195$, $b = 968$.

11.97 Ache: (*a*) mmc (5, 7); (*b*) mmc (3, 33); (*c*) mmc (12, 28).

11.98 Suponha que $a = 5880$ e $b = 8316$.

(*a*) Expresse a e b como produto de primos.

(*b*) Ache mdc (a, b) e mmc (a, b).

(*c*) Verifique que mmc $(a, b) = (|ab|)/\text{mdc}(a, b)$.

11.99 Prove: (*a*) se $a|b$, então $a|-b$, $-a|b$ e $-a|-b$; (*b*) se $ac|bc$, então $b|c$.

11.100 Prove:

(*a*) Se $n > 1$ não é primo, então n tem um divisor positivo d tal que $d \leq \sqrt{n}$.

(*b*) Se $n > 1$ não é divisível por um primo $p \leq \sqrt{n}$, então n é um primo.

11.101 Prove: (*a*) Se $am + bn = 1$, então $\text{mdc}(a, b) = 1$. (*b*) Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

11.102 Prove: (*a*) $\text{mdc}(a, a + k)$ divide k. (*b*) $\text{mdc}(a, a + 2)$ é igual a 1 ou 2.

11.103 Prove:

(*a*) Se $a > 2$ e $k > 1$, então $a^k - 1$ não é primo.

(*b*) Se $n > 0$ e $2^n - 1$ é primo, então n é primo.

11.104 Seja n um inteiro positivo. Prove:

(*a*) 3 divide n se e somente se 3 divide a soma dos dígitos de n.

(*b*) 9 divide n se e somente se 9 divide a soma dos dígitos de n.

(*c*) 8 divide n se e somente se 8 divide o inteiro formado pelos últimos três dígitos de n.

11.105 Estenda a definição de mdc e mmc para qualquer conjunto finito de inteiros, isto é, para inteiros $a_1, a_2, \ldots, a_k$, defina

(*a*) $\text{mdc}(a_1, a_2, \ldots, a_k)$; (*b*) $\text{mmc}(a_1, a_2, \ldots, a_k)$.

11.106 Prove: se $a_1|n$ e $a_2|n, \ldots, a_k|n$, então $m|n$, onde $m = \text{mmc}(a_1, \ldots, a_k)$.

11.107 Prove: existem intervalos arbitrariamente grandes entre números primos, isto é, para qualquer inteiro positivo k, existem k inteiros consecutivos que não são primos.

Congruências

11.108 Quais das seguintes afirmações são verdadeiras?

(*a*) $224 \equiv 762 \pmod 8$ (*b*) $582 \equiv 263 \pmod{11}$ (*c*) $156 \equiv -369 \pmod 7$ (*d*) $-238 \equiv 483 \pmod{13}$

11.109 Ache o menor inteiro não negativo que seja congruente módulo $m = 9$ a cada um dos seguintes números:

(*a*) 457; (*b*) 1578; (*c*) −366; (*d*) −3288.

[O inteiro deve estar no conjunto {0, 1, 2...7, 8}.]

11.110 Ache o menor inteiro não negativo que seja congruente módulo $m = 9$ a cada um dos seguintes números:

(*a*) 511; (*b*) 1329; (*c*) −625; (*d*) −2717.

[O inteiro deve estar no conjunto {−4, −3, −2, −1, 0, 1, 2, 3, 4}.]

Hidden page

(*a*) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$.
(*b*) $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$, $x \equiv 6 \pmod 9$.

11.132 Ache a menor solução positiva do seguinte sistema de equações de congruência.

$$x \equiv 5 \pmod{45}; \quad x \equiv 6 \pmod{49}; \quad x \equiv 7 \pmod{52}$$

Respostas dos Problemas Complementares

11.69 (*a*) $2 > -6$; (*b*) $-3 > -5$; (*c*) $-7 < 3$; (*d*) $-8 < -1$; (*e*) $2^3 < 11$; (*f*) $2^3 > -9$; (*g*) $-2 > -7$; (*h*) $4 > -9$.

11.70 (*a*) 6, 5, 0; (*b*) 4, 4, 10.

11.71 (*a*) $3 + 10 = 13$, $3 - 7 = -4$; (*b*) $4 + 1 = 5$, $8 - 4 = 4$.

11.72 (*a*) 7; (*b*) 9; (*c*) 6; (*d*) 6; (*e*) 6; (*f*) 3.

11.73 (*a*) 4, 5, 6; (*b*) $-2, -1, 0, 1$.

11.88 (*a*) $q = 28$, $r = 3$; (*b*) $q = -15$, $r = 13$; (*c*) $q = -24$, $r = 10$; (*d*) $q = 53$, $r = 7$.

11.90 (*a*) Um é divisível por 2 e o outro é divisível por 3.
(*b*) Um é divisível por 4, outro é divisível por 2, e um é divisível por 3.

11.93 (*a*) 1, 2, 3, 4, 6, 12, 24; (*b*) 3^n para $n = 0$ até 9; (*c*) 2^r3^s para $r = 0$ até 4, e $s = 0$ até 3.

11.94 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

11.95 (*a*) $2940 = 2^2 \cdot 3 \cdot 5 \cdot 7^2$; (*b*) $1485 = 3^3 \cdot 5 \cdot 11$; (*c*) $8712 = 2^3 \cdot 3^2 \cdot 11^2$; (*d*) $319\,410 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13^2$.

11.96 (*a*) $d = 4 = 5(356) - 37(48)$; (*b*) $d = 33 = 8(165) - 1(1287)$; (*c*) $d = 42 = 14(168) - 1(2310)$; (*d*) $d = 1 = 139(195) - 28(968)$.

11.97 (*a*) 35; (*b*) 33; (*c*) 84.

11.98 (*a*) $a = 2^4 \cdot 3 \cdot 5 \cdot 7^2$, $b = 2^2 \cdot 3^3 \cdot 7 \cdot 11$. (*b*) mdc $(a, b) = 2^2 \cdot 3 \cdot 7$, mmc $(a, b) = 2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11$

11.103 (*a*) *Sugestão:* $a^k - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{k-1})$.
(*b*) *Sugestão:* se $n = ab$, então $2^n - 1 = (2^a)^b - 1$.

11.107 $(k + 1)! + 2$, $(k + 1)! + 3$, $(k + 1)! + 4, \ldots,$ $(k + 1)! + (k + 1)$ são divisíveis por 2, 3, 4, $\ldots, k + 1$, respectivamente.

11.108 (*a*) Falso; (*b*) verdadeiro; (*c*) verdadeiro; (*d*) falso.

11.109 (*a*) 7; (*b*) 2; (*c*) 3; (*d*) 6.

11.110 (*a*) -2; (*b*) -3; (*c*) -2; (*d*) 1.

11.111 4, 15, 26, 37, 48, 59, 70, 81, 92.

11.112 $-42, -33, -24, -15, -6, 3, 12, 21, 30, 39, 48$.

11.113 (*a*) $\{0, 1, \ldots, 10\}$ e $\{-5, -4, \ldots, -1, 0, 1, \ldots 4, 5\}$.
(*b*) $\{0, 1, \ldots, 13\}$ e $\{-6, -5, \ldots, -1, 0, 1, \ldots, 6, 7\}$.

11.114 (*a*) $\{1, 3\}$; (*b*) $\{1, 2, \ldots, 10\}$; (*c*) $\{1, 3, 5, 9, 11, 13\}$; (*d*) $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

11.115 (*a*) $\{5, 10, 15, 20, 25, 30, 35, 40\}$; (*b*) $\{3, 9, 27, 81, 243, 729, 2187, 6561\}$.

11.116 $m - 1 \equiv -1 \pmod m$ e, portanto, $(m - 1)^2 \equiv (-1)^2 = 1^2 \pmod m$.

Hidden page

Capítulo 12

Sistemas Algébricos

12.1 INTRODUÇÃO

Esta seção investiga alguns dos sistemas algébricos mais importantes em matemática: semigrupos, grupos, anéis e corpos. Definimos também as noções de homomorfismo e estrutura de quocientes. Iniciamos com a definição formal de operação e discutimos seus vários tipos.

12.2 OPERAÇÕES

O leitor está familiarizado com as operações de adição e multiplicação de números, união e interseção de conjuntos e composição de funções. Essas operações são denotadas como a seguir:

$$a + b = c, \qquad a \cdot b = c, \qquad A \cup B = C, \qquad A \cap B = C, \qquad g \circ f = h.$$

Em cada situação, um elemento (c, C ou h) é associado ao par original de elementos. Em outras palavras, existe uma função que associa um único elemento a um par de elementos dado. Tornaremos precisa, agora, essa noção.

Definição: Seja S um conjunto não vazio. Uma *operação* em S é uma função $*$ de $S \times S$ em S. Neste caso, escrevemos normalmente

$$a * b \quad \text{ou, às vezes,} \quad ab$$

em vez de $*$ (a,b). O conjunto S, juntamente com a operação $*$ em S, é denotado pela estrutura $(S, *)$ ou, simplesmente, S quando a operação é subentendida.

Observação: Uma operação $*$ de $S \times S$ em S é geralmente chamada *operação binária*. Uma operação *unária* é uma função de S para S. Por exemplo, o valor absoluto $|n|$ de um inteiro n é uma operação unária em $\mathbf{Z}$, e o complementar, A^c, de um conjunto A é uma operação unária no conjunto das partes de X, $P(X)$. Uma operação *ternária* (3-ária) é uma função de $S \times S \times S$ em S. Mais genericamente, uma operação *n-ária* é uma função de $S \times S \times \ldots \times S$ (n vezes) em S. A menos que haja afirmação em contrário, a palavra operação significará operação binária. Também vamos supor que o conjunto S é não vazio.

Suponha que S é um conjunto finito. Então, uma operação pode ser descrita pela sua tabela onde o elemento na posição da linha rotulada por a e da coluna rotulada por b é $a * b$.

Suponha que S é um conjunto com uma operação $*$, e suponha que A é um subconjunto de S. Então A é dito *fechado sob* $*$ se, para todo a e b em A, $a * b$ pertence a A.

Hidden page

Teorema 12-1: suponha que $*$ é uma operação associativa em um conjunto S. Então, todo produto $a_1 * a_2 * \cdots * a_n$ dispensa o uso de parênteses, isto é, todas as possibilidades são iguais.

Uma operação $*$ em um conjunto S é *comutativa* ou satisfaz a *lei da comutatividade* se

$$a * b = b * a$$

para quaisquer elementos a, b em S.

Exemplo 12.4

(*a*) Considere o conjunto **Z** dos inteiros. Adição e multiplicação de inteiros são associativas e comutativas. Por outro lado, subtração não é associativa. Por exemplo,

$$(8-4)-3=1 \qquad \text{mas} \qquad 8-(4-3)=7$$

Além disto, a subtração é não comutativa pois, por exemplo, $3-7 \neq 7-3$.

(*b*) Considere a operação de multiplicação de matrizes no conjunto M de matrizes quadradas $n \times n$. Pode-se mostrar (Seção 5.5) que a multiplicação de matrizes é associativa. Por outro lado, a multiplicação de matrizes não é comutativa. Por exemplo,

$$\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\begin{bmatrix}5 & 6\\ 0 & -2\end{bmatrix}=\begin{bmatrix}5 & 2\\ 15 & 10\end{bmatrix} \qquad \text{mas} \qquad \begin{bmatrix}5 & 6\\ 0 & -2\end{bmatrix}\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}=\begin{bmatrix}23 & 34\\ -6 & -8\end{bmatrix}$$

(*c*) Considere a operação exponencial $a * b = a^b$ no conjunto **N** de inteiros positivos. A operação não é associativa. Por exemplo,

$$(2*2)*3=(2^2)^3=4^3=64 \qquad \text{mas} \qquad 2*(2*3)=2^{2^3}=2^8=256$$

Além disto, $*$ não é comutativa. Por exemplo,

$$2*3=2^3=8 \qquad \text{mas} \qquad 3*2=3^2=9$$

(*d*) Considere a operação em $S = \{a, b, c, d\}$ definida pela tabela na Figura 12-1(*b*). A operação não é associativa. Por exemplo,

$$(b \cdot c) \cdot c = a \cdot c = c \qquad \text{mas} \qquad b \cdot (c \cdot c) = b \cdot a = b$$

Além disso, a operação não é comutativa. Por exemplo, $b \cdot c = a$, mas $c \cdot b = b$.

(2) **Elemento identidade e inversos**

Considere uma operação $*$ em um conjunto S. Um elemento e em S é dito um elemento *identidade* para $*$ se, para qualquer elemento a em S,

$$a * e = e * a = a$$

Mais genericamente, um elemento e em S é dito uma *identidade à esquerda* ou uma *identidade à direita*, dependendo de $e * a = a$ ou $a * e = a$, onde a é um elemento qualquer de S. O teorema seguinte pode ser aplicado.

Teorema 12-2: suponha que e é uma identidade à esquerda, e f é uma identidade à direita para uma operação em um conjunto S. Então, $e = f$.

A demonstração é muito simples. Como e é uma identidade à esquerda, $ef = f$; mas como f é uma identidade à direita, $ef = e$. Logo, $e = f$. Esse teorema nos diz, em particular, que um elemento identidade é único e que, se uma operação tem mais de uma identidade à esquerda, então ela não tem identidade à direita e vice-versa.

Suponha que uma operação $*$ em um conjunto S tem um elemento identidade e. O inverso de um elemento a em S é um elemento b tal que

$$a * b = b * a = e$$

Se a operação é associativa, o inverso de a, se existir, é único (Problema 12.3). Observe que, se b é o inverso de a, a é o inverso de b. Portanto, o inverso define uma relação de simetria, e podemos dizer que os elementos a e b são inversos.

Notação: se a operação em S é denotada por $a * b$, $a \times b$, $a \cdot b$ ou ab, então dizemos que S é descrito *multiplicativamente*, e o inverso de um elemento a em S é denotado normalmente por a^{-1}. Às vezes, quando S é comutativo, a operação é denotada por $+$, e diz-se que S é descrito *aditivamente*. Neste caso, o elemento identidade é normalmente denotado por 0 e é chamado elemento *zero*; o inverso é denotado por $-a$ e é chamado *negativo* de a.

Exemplo 12.5

(*a*) Considere os números racionais **Q**. Sob adição, 0 é o elemento identidade, e -3 e 3 são inversos (aditivos), já que

$$(-3) + 3 = 3 + (-3) = 0$$

Por outro lado, sob a operação de multiplicação, 1 é o elemento identidade, e -3 e $-\frac{1}{3}$ são inversos (multiplicativos), pois

$$(-3) \cdot \left(-\frac{1}{3}\right) = \left(-\frac{1}{3}\right) \cdot (-3) = 1$$

Note que 0 não tem inverso multiplicativo.

(*b*) Considere o conjunto $S = \{a, b, c, d\}$ munido da operação definida pela Figura 12-1(*b*). Note que o elemento a é um elemento identidade. Note também que $dd = a$, e assim d é seu próprio inverso. Ademais, $dc = cd = a$ e, portanto, c e d são também inversos um do outro. Logo, o inverso de d não é único. (Isso implica que a operação não pode ser associativa.)

(3) **Leis de cancelamento**

Diz-se que uma operação $*$ em um conjunto S satisfaz a *lei do cancelamento à esquerda* se

$$a * b = a * c \text{ implicar } b = c$$

e satisfaz a *lei do cancelamento à direita* se

$$b * a = c * a \text{ implicar } b = c$$

Adição e subtração de inteiros em **Z** e multiplicação de inteiros não nulos em **Z** satisfazem as leis do cancelamento, direita e esquerda. Por outro lado, a multiplicação de matrizes não satisfaz as leis do cancelamento. Por exemplo, suponha

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad C = \begin{bmatrix} 0 & -3 \\ 1 & 5 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$$

Então, $AB = AC = D$, mas $B \neq C$.

12.3 SEMIGRUPOS

Seja S um conjunto não vazio com uma operação. Então, S é dito um *semigrupo* se a operação é associativa. Se a operação também tem um elemento identidade, então S é dito um *monóide*.

Exemplo 12.6

(*a*) Considere os inteiros positivos **N**. Então, (**N**, +) e (**N**, ×) são semigrupos, pois adição e multiplicação em **N** são associativas. Em particular, (**N**, ×) é um monóide, pois existe o elemento identidade 1. Entretanto, (**N**,+) não é um monóide, já que adição em **N** não tem o elemento zero.

(*b*) Seja S um conjunto finito e $F(S)$ a coleção de todas as funções $f: S \to S$ munida da operação de composição de funções. Como a composição de funções é associativa, $F(S)$ é um semigrupo. De fato, $F(S)$ é um monóide, já que a função identidade é um elemento identidade em $F(S)$.

(*c*) Seja $S = \{a, b, c, d\}$. As tabelas de multiplicação na Figura 12-1 definem operações $*$ e $\cdot$ em S. Note que $*$ pode ser definido pela fórmula $x * y = x$ para todo x e y em S. Portanto,

$$(x * y) * z = x * z = x \qquad \text{e} \qquad x * (y * z) = x * y = x$$

Portanto, $*$ é associativa e, logo, $(S, *)$ é um semigrupo. Por outro lado, $\cdot$ não é associativa, já que, por exemplo,

$$(b \cdot c) \cdot c = a \cdot c = c \qquad \text{mas} \qquad b \cdot (c \cdot c) = b \cdot a = b$$

Logo, $(S, \cdot)$ não é um semigrupo.

Semigrupo Livre, Monóide Livre

Seja A um conjunto não vazio. Uma *palavra* w em A é uma seqüência finita de elementos de A. Por exemplo,

$$u = ababbbb = abab^4 \qquad \text{e} \qquad v = baccaaaa = bac^2a^4$$

são palavras em $A = \{a, b, c\}$. (Escrevemos a^2 para aa, a^3 para aaa, e assim por diante.) O comprimento de uma palavra w, denotado por $l(w)$, é o número de elementos em w. Portanto, $l(u) = 7$ e $l(v) = 8$.

A *concatenação* de palavras u e v em um conjunto A, denotada por $u * v$ ou uv, é a palavra obtida quando se escreve os elementos de u seguidos pelos elementos de v. Por exemplo,

$$uv = (abab^4)(bac^2a^4) = abab^5c^2a^4$$

Agora, seja $F = F(A)$ a coleção de todas as palavras em A munidas da operação de concatenação. Claramente, para quaisquer palavras u, v e w, as palavras $(uv)w$ e $u(vw)$ são idênticas. Elas consistem simplesmente nos elementos de u, v e w escritos um após o outro. Portanto, F é um semigrupo; ele é dito o *semigrupo livre* em A, e os elementos de A são os *geradores* de F.

A seqüência vazia, denotada por λ, também é considerada uma palavra em A. Entretanto, não assumimos que λ pertence ao semigrupo livre $F = F(A)$. O conjunto de todas as palavras em A, incluindo λ, é denotado, freqüentemente, por A^*. Logo, A^* é um monóide sob a operação de concatenação; é chamado monóide livre em A.

Subsemigrupos

Seja A um subconjunto não-vazio de um semigrupo S. A é dito um *subsemigrupo* de S se o próprio A é um semigrupo munido da operação definida em S. Como os elementos de A também são elementos definidos em S, a lei associativa vale automaticamente para os elementos de A. Portanto, A é um subsemigrupo de S se e somente se A é fechado sob a operação em S.

Exemplo 12.7

(*a*) Denote por A e B, respectivamente, os conjuntos de pares e ímpares nos inteiros positivos. Então, $(A, \times)$ e $(B, \times)$ são subsemigrupos de $(\mathbf{N}, \times)$, pois A e B são fechados sob a operação de multiplicação. Por outro lado, $(A, +)$ é um subsemigrupo de $(\mathbf{N}, +)$, já que A é fechado sob a operação de adição, mas $(B, +)$ não é um subsemigrupo de $(\mathbf{N}, +)$, já que B não é fechado sob adição.

(*b*) Considere o semigrupo livre F em um conjunto $A = \{a, b\}$. Seja H o conjunto de todas as palavras *pares*, isto é, palavras de comprimento par. A concatenação de duas tais palavras também é par. Portanto, H é um subsemigrupo de F.

Relações de Congruência e Estruturas de Quociente

Seja S um semigrupo, e seja $\sim$ uma relação de equivalência em S. Lembre que a relação de equivalência $\sim$ induz uma partição de S em classes de equivalência, onde $[a]$ denota a classe de equivalência contendo o elemento a de S, e que a coleção de classes de equivalência é denotada por $S/\sim$.

Suponha que a relação de equivalência $\sim$ em S tem a seguinte propriedade:

Se $a \sim a'$ e $b \sim b'$ então $ab \sim a'b'$.

Então, $\sim$ é dita uma *relação de congruência* em S. Além do mais, podemos agora definir uma operação nas classes de equivalência por

$$[a] * [b] = [a * b] \qquad \text{ou simplesmente} \qquad [a][b] = [ab]$$

Além disso, esta operação em $S/\sim$ é associativa; portanto, $S/\sim$ é um semigrupo. Formalizamos esse resultado a seguir.

Teorema 12-3: seja $\sim$ uma relação de congruência em um semigrupo S. Então $S/\sim$, o conjunto das classes de equivalência induzidas por $\sim$, forma um semigrupo sob a operação

$$[a][b] = [ab]$$

Este semigrupo é chamado de *quociente* de S por $\sim$.

Hidden page

Logo, a função determinante define um homomorfismo de semigrupos em $(M, \times)$, as matrizes sob a operação de multiplicação. Por outro lado, a função determinante não é aditiva, isto é, para algumas matrizes,

$$\det(A + B) \neq \det(A) + \det(B)$$

Logo, a função determinante não define um homomorfismo de semigrupos em $(M,+)$.

(*d*) Seja ~ uma relação de congruência em um semigrupo S. Seja ϕ: $S \to S/\sim$ o *mapeamento natural* de S no semigrupo quociente $S/\sim$ definido por

$$\phi(a) = [a]$$

Isto é, cada elemento a em S é associado à sua classe de equivalência $[a]$. Então ϕ é um homomorfismo, pois

$$\phi(ab) = [ab] = [a][b] = \phi(a)\phi(b)$$

Teorema Fundamental de Homomorfismos de Semigrupos

Lembre que a imagem de uma função f: $S \to S'$, denotada por $f(S)$ ou Im f, consiste nas imagens dos elementos de f por S; isto é,

$$\text{Im } f = \{b \in S' : \text{existe } a \in S \text{ para o qual } f(a) = b\}$$

O teorema seguinte (provado no Problema 12.8) é fundamental para a teoria de semigrupos.

Teorema 12-4: seja f: $S \to S'$ um homomorfismo de semigrupos. Defina $a \sim b$ se $f(a) = f(b)$. Então:
(i) ~ é uma relação de congruência em S.
(ii) $S/\sim$ é isomorfo a $f(S)$.

Exemplo 12.10

(*a*) Seja F o semigrupo livre em $A = \{a, b\}$. A função f: $F \to \mathbf{Z}$ definida por

$$f(u) = \ell(u)$$

é um homomorfismo. Note que $f(F) = \mathbf{N}$. Logo, $F/\sim$ é isomorfo a $\mathbf{N}$.

(*b*) Seja M o conjunto das matrizes 2×2 com elementos inteiros. Considere a função det: $M \to \mathbf{Z}$. Para qualquer inteiro a, temos

$$\det\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = a$$

Logo, a imagem de determinante é $\mathbf{Z}$. Pelo Teorema 12.4, $M/\sim$ é isomorfo a $\mathbf{Z}$.

Produtos de Semigrupos

Sejam $(S_1, *_1)$ e $(S_2, *_2)$ semigrupos. Formamos um novo semigrupo $S = S_1 \otimes S_2$, chamado *produto direto* de S_1 e S_2, como descrito a seguir.

(1) Os elementos de S vêm de $S_1 \times S_2$, isto é, os elementos de S são pares ordenados (a, b) onde $a \in S_1$ e $b \in S_2$.

(2) A operação $*$ em S é definida componente a componente, isto é,

$$(a, b) * (a', b') = (a *_1 a', b *_2 b') \qquad \text{ou simplesmente} \qquad (a, b)(a', b') = (aa', bb')$$

Pode-se mostrar facilmente (por exemplo, como no Problema 12.5(*a*)) que a operação acima é associativa.

12.4 GRUPOS

Seja G um conjunto não vazio com uma operação binária (denotada por justaposição). Então G é dito um grupo se os seguintes axiomas valem:

$[\mathbf{G}_1]$ *Lei associativa*: para todo a, b, c em G, temos $ab(c) = a(bc)$.
$[\mathbf{G}_2]$ *Elemento identidade*: existe um elemento e em G tal que $ae = ea = a$ para todo a em G.
$[\mathbf{G}_3]$ *Inversos*: para cada a em G, existe um elemento a^{-1} em G (o *inverso* de a) tal que

$$aa^{-1} = a^{-1}a = e$$

Um grupo G é dito *abeliano* (ou *comutativo*) se vale a propriedade de comutatividade . Isto é, $ab = ba$ para todo $a, b \in G$.

Quando a operação binária é denotada por justaposição, como há pouco, diz-se que o grupo G está descrito de forma *multiplicativa*. Às vezes, quando G é abeliano, a operação binária é denotada por +, e diz-se que G está descrito *aditivamente*. Neste caso, o elemento identidade é denotado por 0 e é denominado elemento *zero*; o inverso é denotado por $-a$ e é chamado de *negativo* de a.

O número de elementos de um grupo G, denotado por $|G|$, é chamado *ordem* de G, e G é dito um *grupo finito* se sua ordem é finita. Se A e B são subconjuntos de G, escrevemos

$$AB = \{ab: a \in A, b \in B\} \qquad \text{ou} \qquad A + B = \{a + b: a \in A, b \in B\}$$

Exemplo 12.11

(*a*) O conjunto $\mathbf{Z}$ dos inteiros é um grupo abeliano sob adição. O elemento identidade é 0, e $-a$ é o inverso aditivo de a em $\mathbf{Z}$.

(*b*) Os números racionais não nulos $Q\backslash\{0\}$ formam um grupo abeliano sob a operação de multiplicação. O número 1 é a identidade, e o elemento q/p é o inverso multiplicativo de p/q.

(*c*) Seja S o conjunto das matrizes 2×2 com elementos racionais sob a operação de multiplicação de matrizes. Então S não é um grupo, já que os inversos não existem sempre. Entretanto, seja G o subconjunto das matrizes 2×2 com determinante não nulo. Então, G é um grupo sob a operação de multiplicação de matrizes. O elemento identidade é

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e o inverso de } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ é } A^{-1} = \begin{pmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{pmatrix}.$$

Esse é um exemplo de um grupo não abeliano, já que multiplicação de matrizes não é comutativa.

(*d*) Lembre que $\mathbf{Z}_m$ denota os inteiros módulo m. $\mathbf{Z}_m$ é um grupo sob adição, mas não é um grupo sob a multiplicação. Entretanto, seja $\mathbf{U}_m$ um sistema reduzido de resíduos módulo m consistindo nos inteiros primos relativos de m. Então $\mathbf{U}_m$ é um grupo sob a operação de multiplicação (mod m). Por exemplo, a Figura 12-3 mostra a tabela de multiplicação para $\mathbf{U}_{12} = \{1, 5, 7, 11\}$.

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Fig. 12-3

	ϵ	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
ϵ	ϵ	σ_1	σ_2	σ_3	ϕ_1	ϕ_2
σ_1	σ_1	ϵ	ϕ_1	ϕ_2	σ_2	σ_3
σ_2	σ_2	ϕ_2	ϵ	ϕ_1	σ_3	σ_1
σ_3	σ_3	ϕ_1	ϕ_2	ϵ	σ_1	σ_2
ϕ_1	ϕ_1	σ_3	σ_1	σ_2	ϕ_2	ϵ
ϕ_2	ϕ_2	σ_2	σ_3	σ_1	ϵ	ϕ_1

Fig. 12-4

Grupo Simétrico S_n

Um mapeamento um-a-um σ do conjunto $\{1, 2, \ldots, n\}$ em si mesmo é dito uma permutação. Uma tal permutação é denotada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix}$$

onde $j_i = \sigma(i)$.

O conjunto de todas as *permutações* deste tipo é denotado por S_n, e existem $n! = 1 \cdot 2 \cdot \cdots \cdot n$ delas. A composição de permutações e a inversa de permutações em S_n pertencem a S_n, e a função identidade e pertence a S_n. Portanto, S_n forma um grupo sob a composição de funções que é chamado *grupo simétrico de grau n*.

O grupo simétrico S_3 tem $3! = 6$ elementos como a seguir:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

A tabela de multiplicação de S_3 aparece na Figura 12-4.

MAP(*A*), PERM(*A*) e AUT(*A*)

Seja A um conjunto não vazio. A coleção MAP(A) de todas as funções (mapeamentos) $f: A \to A$ é um semigrupo sob a composição de funções; não é um grupo, pois algumas funções não têm inversas. Entretanto, o semigrupo PERM(A), contendo todas as correspondências bijetoras de A em si mesmo (chamado *permutações* de A), é um grupo sob a composição de funções.

Além disso, suponha que A contém algum tipo de estrutura geométrica ou algébrica; por exemplo, A pode ser o conjunto de vértices de um grafo, ou um conjunto ordenado ou um semigrupo. Então, o conjunto AUT(A) de todos os isomorfismos de A em si mesmo (chamados *automorfismos* de A) também é um grupo sob a composição de funções.

12.5 SUBGRUPOS, SUBGRUPOS NORMAIS E HOMOMORFISMOS

Seja H um subconjunto de um grupo G. Então H é dito um *subgrupo* de G se H é, em si, um grupo sob a operação de G. Apresentamos a seguir critérios simples para determinar subgrupos.

Proposição 12.5: um subconjunto H de um grupo G é um subgrupo de G se:
(i) o elemento identidade $e \in H$;
(ii) H é fechado sob a operação de G, i.e., $a, b \in H$, então $ab \in H$;
(iii) H é fechado sob inversos, isto é, se $a \in H$, então $a^{-1} \in H$.

Todo grupo G tem $\{e\}$ e o próprio G como subgrupos. Qualquer outro subgrupo de G é dito um *subgrupo não trivial*.

Classes Laterais

Se H é um subgrupo de G e $a \in G$, então o conjunto

$$Ha = \{ha: h \in H\}$$

é chamado *classe lateral à direita* de H. (Analogamente, aH é chamado *classe lateral à esquerda* de H.) Temos os seguintes resultados importantes (provados no Problema 12.17 e 12.19).

Teorema 12-6: seja H um subgrupo de um grupo G. Então, as classes laterais à direita Ha formam uma partição de G.

Teorema 12-7: (**Lagrange**) seja H um subgrupo de um grupo finito G. Então a ordem de H divide a ordem de G.

Na verdade, é possível mostrar que o número de classes laterais à direita de H em G, chamado *índice* de H em G, é igual ao número de classes laterais à esquerda de H em G; ambos os números são iguais a $|G|$ dividido por $|H|$.

Subgrupos Normais

Apresentamos a seguinte definição.

Definição: Um subgrupo H de G é um subgrupo *normal* se $a^{-1}Ha \subseteq H$ para todo a em G. Equivalentemente, H é normal se $aH = Ha$ para todo $a \in G$, i.e., se as classes laterais à direita e à esquerda coincidem.

Note que todo subgrupo de um grupo abeliano é normal.

A importância dos subgrupos normais vem do resultado seguinte (provado no Problema 12.24).

Teorema 12-8: seja H um subgrupo normal de um grupo G. Então, as classes laterais de H formam um grupo sob a operação de multiplicação de classes laterais.

$$(aH)(bH) = abH$$

Esse grupo é chamado de grupo quociente e é denotado por G/H.

Suponha que a operação em G seja adição ou, em outras palavras, G seja descrito aditivamente. Então, as classes laterais de um subgrupo H de G são da forma $a + H$. Além disso, se H é um subgrupo normal de G, então as classes laterais formam um grupo sob a adição de classes laterais, isto é

$$(a + H) + (b + H) = (a + b) + H$$

Exemplo 12.12

(*a*) Considere o grupo de permutações de grau 3, S_3, que foi estudado ateriormente. O conjunto $H = \{e, \sigma_1\}$ é um subgrupo de S_3. Suas classes laterais à esquerda e direita são:

Classes laterais à direita	Classes laterais à esquerda
$H = \{e, \sigma_1\}$	$H = \{e, \sigma_1\}$
$H\phi_1 = \{\phi_1, \sigma_2\}$	$\phi_1 H = \{\phi_1, \sigma_3\}$
$H\phi_2 = \{\phi_2, \sigma_3\}$	$\phi_2 H = \{\phi_2, \sigma_2\}$

Observe que as classes laterais à esquerda e à direita são distintas; portanto, H não é um subgrupo normal de S_3.

(*b*) Considere o grupo G de matrizes 2×2 com elementos racionais e determinante não nulo. [Veja o Exemplo 12.11(*c*)]. Seja H o subconjunto de G consistindo nas matrizes cujo elemento superior direito é zero; i.e., matrizes da forma

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

Então, H é um subgrupo de G, pois H é fechado sob multiplicação e inversos e $I \in H$. Entretanto, H não é um subgrupo normal pois, por exemplo,

$$\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & -4 \\ 1 & 3 \end{pmatrix}$$

não pertence a H.

Por outro lado, seja K o subconjunto de G formado pelas matrizes de determinante 1. Pode-se mostrar que K também é um subgrupo de G. Além disso, para qualquer matriz X em G e qualquer matriz A em K, temos

$$\det(X^{-1}AX) = 1$$

Portanto, $X^{-1}AX$ pertence a K, e K é um subgrupo normal de G.

Inteiros Módulo *m*

Considere o grupo G, dos inteiros sob adição. Denote por H os múltiplos de 5, isto é,

$$H = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

Então, H é um subgrupo (necessariamente normal) de $\mathbf{Z}$. As classes laterais de H em $\mathbf{Z}$ são:

$$\begin{aligned}
\bar{0} &= 0 + H = H = \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
\bar{1} &= 1 + H = \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
\bar{2} &= 2 + H = \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
\bar{3} &= 3 + H = \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
\bar{4} &= 4 + H = \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

Pelo Teorema 12.8 acima, $\mathbf{Z}/H = \{0, 1, 2, 3, 4\}$ é um grupo sob a adição de classes laterais; sua tabela aparece na Figura 12-5.

Hidden page

para todo $a, b \in G$. Ademais, se f for bijetor, então f é dito um isomorfismo, e diz-se que G e G' são isomorfos escrevendo-se $G \simeq G'$.

Se $f: G \to G'$ é um homomorfismo, então, o *kernel*[†] de f, denotado por Ker f, é o conjunto de elementos cuja imagem é o elemento identidade de G', e'; isto é

$$\text{Ker}\, f = \{a \in G : f(a) = e'\}$$

Lembre que a imagem de f, denotada por $f(G)$ ou Im f, consiste no conjunto das imagens dos elementos por f, isto é,

$$\text{Im}\, f = \{b \in G' : \text{existe e } a \in G \text{ tal que } f(a) = b\}$$

O teorema seguinte (provado no Problema 12.21) é fundamental para a teoria de grupos.

Teorema 12-9: seja $f: G \to G'$ um homomorfismo com *kernel* K. Então K é um subgrupo normal de G, e o grupo quociente G/K é isomorfo a $f(G)$.

Exemplo 12.13

(*a*) Seja G o grupo dos números reais munidos da operação de adição, e seja G' o grupo dos números reais positivos sob a multiplicação. O mapeamento $f: G \to G'$ definido por $f(a) = 2^a$ é um homomorfismo porque

$$f(a + b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$$

De fato, f também é bijetor; portanto, G e G' são isomorfos.

(*b*) Seja G o grupo dos números complexos diferentes de zero com a operação de multiplicação. O mapeamento $f: G \to G'$ definido por $f(z) = |z|$ é um homomorfismo porque

$$f(z_1 z_2) = |z_1 z_2| = |z_1|\ |z_2| = f(z_1)f(z_2)$$

O *kernel* K de f é composto pelos números complexos z no círculo unitário, i.e., $|z| = 1$. Portanto, G/K é isomorfo à imagem de f, i.e., ao grupo de números reais positivos sob a multiplicação.

(*c*) Seja a um elemento qualquer em um grupo G. A função $f: \mathbf{Z} \to G$ definida por $f(n) = a^n$ é um homomorfismo, pois

$$f(m + n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$$

A imagem de f é $gp(a)$, o subgrupo cíclico gerado por a. Pelo Teorema 12-9,

$$gp(a) \simeq \mathbf{Z}/K$$

onde K é o *kernel* de f. Se $K = \{0\}$, então $gp(a) \simeq \mathbf{Z}$. Por outro lado, se m é a ordem de a, então $K = \{\text{múltiplos de } m\}$ e, portanto, $gp(a) \simeq \mathbf{Z}_m$. Em outras palavras, qualquer grupo cíclico é isomorfo ou aos inteiros $\mathbf{Z}$ sob adição, ou a $\mathbf{Z}_m$, os inteiros sob adição módulo m.

12.6 ANÉIS, DOMÍNIOS INTEGRAIS E CORPOS

Seja R um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por justaposição). Então R é dito um *anel* se são satisfeitos os seguintes axiomas:

- $[\mathbf{R}_1]$ Para cada $a, b, c \in R$, $(a + b) + c = a + (b + c)$.
- $[\mathbf{R}_2]$ Existe um elemento $0 \in R$, chamado elemento *zero*, tal que $a + 0 = 0 + a = a$ para todo $a \in R$.
- $[\mathbf{R}_3]$ Para cada $a \in R$, existe um elemento $-a \in R$, chamado de *negativo de* a, tal que $a + (-a) = (-a) + a = 0$.
- $[\mathbf{R}_4]$ Para todo $a, b \in R$, $a + b = b + a$
- $[\mathbf{R}_5]$ Para todo $a, b, c \in R$, temos $(ab)c = a(bc)$.
- $[\mathbf{R}_6]$ Para todo $a, b, c \in R$, temos (i) $a(b + c) = ab + ac$ e (ii) $(b + c)\, a = ba + ca$.

Observe que os axiomas $[\mathbf{R}_1]$ até $[\mathbf{R}_4]$ podem ser resumidos pela afirmação de que R é um grupo abeliano sob adição.

[†] N. de T. Optamos pelo uso do termo original *kernel*, como é freqüente em textos em português. Quando o termo é traduzido, normalmente usa-se a palavra núcleo.

A subtração é definida em R por $a - b \equiv a + (-b)$.

É possível provar que (veja o Problema 12.29) $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in R$.

Um subconjunto S de R é um *subanel* de R se S for, por si, um anel sob as operações de R. Notamos que S é um subanel de R se (i) $0 \in S$ e (ii) para todo $a, b \in S$, temos $a - b \in S$ e $ab \in S$.

Tipos Especiais de Anéis: Domínios Integrais e Corpos

Esta subseção define alguns tipos especiais de anéis, incluindo domínios integrais e corpos.

R é dito um *anel comutativo* se $ab = ba$ para todo $a, b \in R$.

R é dito um *anel com elemento identidade* 1 se o elemento 1 satisfaz $a \cdot 1 = 1 \cdot a = a$ para todo elemento $a \in R$. Neste caso, um elemento $a \in R$ é uma *unidade* se a tem um *inverso multiplicativo*, isto é, um elemento a^{-1} em R tal que $aa^{-1} = a^{-1}a = 1$.

R é dito um *anel com divisores de zero* se tem elementos não nulos a e $b \in R$ tais que $ab = 0$. Neste caso, a e b são chamados *divisores de zero*.

Definição: Um anel comutativo R é um *domínio integral* se R não tem divisores de zero; isto é, se $ab = 0$ implica $a = 0$ ou $b = 0$.

Definição: Um anel comutativo R com elemento identidade 1 (diferente de 0) é um *corpo* se todo $a \in R$, $a \neq 0$ é uma unidade, isto é, tem inverso multiplicativo.

Um corpo é necessariamente um domínio integral pois, se $ab = 0$ e $a \neq 0$, então

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0$$

Observamos que um corpo também pode ser entendido como um anel comutativo no qual os elementos não nulos formam um grupo sob a multiplicação.

Exemplo 12.14

(*a*) O conjunto $\mathbf{Z}$ dos inteiros com as operações usuais de adição e multiplicação é o exemplo clássico de domínio integral (com um elemento identidade). As unidades em $\mathbf{Z}$ são apenas 1 e –1, isto é, nenhum outro elemento em $\mathbf{Z}$ tem um inverso multiplicativo.

(*b*) O conjunto $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ munido da operação de adição e multiplicação módulo m é um anel; ele é conhecido como o *anel dos inteiros módulo m*. Se m é um primo, $\mathbf{Z}_m$ é um corpo. Por outro lado, se m não é um primo, $\mathbf{Z}_m$ tem divisores de zero. Por exemplo, no anel $\mathbf{Z}_6$,

$$2 \cdot 3 = 0 \qquad \text{mas} \qquad 2 \neq 0 \pmod 6 \qquad \text{e} \qquad 3 \neq 0 \pmod 6$$

(*c*) Os números racionais $\mathbf{Q}$ e os números reais $\mathbf{R}$ formam, cada um, um corpo em relação às operações usuais de adição e multiplicação.

(*d*) Seja M o conjunto das matrizes 2×2 com elementos reais ou inteiros. Então M, munido das operações usuais de soma e multiplicação de matrizes, é um anel não comutativo com divisores de zero. M tem um elemento identidade, a matriz identidade.

(*e*) Seja R um anel qualquer. O conjunto $R[x]$ de todos os polinômios sobre R, munido das operações usuais de adição e multiplicação de polinômios, é um anel. Além disso, se R é um domínio integral, $R[x]$ é um domínio integral.

Ideais

Um subconjunto J de um anel R é dito um *ideal* em R se valem as seguintes três propriedades:

(i) $0 \in J$.

(ii) Para todo $a, b \in J$, temos $a - b \in J$.

(iii) Para todo $r \in \mathbf{R}$ e $a \in J$, temos $ra, ar \in J$.

Note primeiramente que J é um subanel de R. Além disso, J é um subgrupo (necessariamente normal) do grupo aditivo R. Assim, podemos formar a coleção de classes laterais

$$\{a + J : a \in R\}$$

que formam uma partição de R.

A importância dos ideais vem do teorema seguinte, que é análogo ao Teorema 12.7 para subgrupos normais.

Teorema 12-10: seja J um ideal em um anel R. Então as classes laterais $\{a + J: a \in \mathbf{R}\}$ formam um anel quando munidas das operações

$$(a + J) + (b + J) = a + b + J \qquad \text{e} \qquad (a + J)(b + J) = ab + J$$

Esse anel é denotado por R/J e é dito o *anel quociente*.

Seja R um anel comutativo com elemento identidade 1. Para todo $a \in R$, o conjunto $(a) = \{ra: r \in R\} = aR$ é um ideal; ele é dito o *ideal principal* gerado por a. Se todo ideal em R é um ideal principal, então R é dito um *anel ideal principal*. Em particular, se R também é um domínio integral, então R é chamado *domínio ideal principal* (DIP).

Exemplo 12.15

(*a*) Considere o anel $\mathbf{Z}$ dos inteiros. Todo ideal J em $\mathbf{Z}$ é um ideal principal. Isto é, $J = (m) = m\mathbf{Z}$, para algum inteiro m. Portanto, $\mathbf{Z}$ é um *domínio ideal principal* (DIP). O anel quociente $\mathbf{Z}_m = \mathbf{Z}/(m)$ é simplesmente o anel dos inteiros módulo m. Embora $\mathbf{Z}$ seja um domínio integral (não contém divisores de zero), o anel quociente $\mathbf{Z}_m$ pode ter divisores de zero, por exemplo, 2 e 3 são divisores de zero em $\mathbf{Z}_6$.

(*b*) Seja R um anel qualquer. Então $\{0\}$ e R são ideais. Em particular, se R é um corpo, $\{0\}$ e R são os únicos ideais.

(*c*) Seja K um corpo. Então, o anel $K[x]$ de polinômios sobre K é um domínio ideal principal (DIP). Por outro lado, o anel $K[x,y]$ de polinômios em duas variáveis não é um DIP.

(*d*) Seja M o anel das matrizes 2×2 com elementos inteiros. Defina J como o conjunto das matrizes da forma

$$\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$$

Note que (i) $0 \in J$. (ii) Para todo $a, b \in J$, temos $a - b \in J$. (iii) Para todo r em M e a em J, temos $ra \in J$; isto é, $RJ \subseteq J$. Entretanto, $JR \not\subseteq J$. Logo, J não é um ideal. (Ele é dito um *ideal à esquerda*).

Homomorfismos de Anéis

Uma função f de um anel R em um anel R' é dita um *homomorfismo de anéis* ou, simplesmente, um *homomorfismo* se

$$f(a + b) = f(a) + f(b), \qquad f(ab) = f(a)f(b)$$

para todo $a, b \in R$. Se f também é bijetora, f é dita um *isomorfismo* e diz-se que R e R' são *isomorfos*; denota-se $R \simeq R'$.

Se $f: R \to R'$ é um homomorfismo, então o núcleo de f, denotado por $\text{Ker}\, f$, é o conjunto de elementos cuja imagem é o zero de R'; isto é

$$\text{Ker}\, f = \{r \in R: f(r) = 0\}$$

O teorema seguinte (análogo ao Teorema 12.9 para grupos) é fundamental para a teoria de anéis.

Teorema 12-11: seja $f: R \to R'$ um homomorfismo de anéis com núcleo K. Então K é um ideal em R, e o anel quociente R/K é isomorfo a $f(R)$.

Divisibilidade e Domínios Integrais

Seja D um domínio integral. Dizemos que b *divide* a em D se $a = bc$ para algum $c \in D$. Um elemento u em D é dito uma unidade se u divide 1, i.e., se u tem um inverso multiplicativo. Um elemento b em d é dito um *associado* de $a \in D$ se $b = ua$ para alguma unidade $u \in D$. Um elemento que não é uma unidade $p \in D$ é dito *irredutível* se $p = ab$ implica que a ou b é uma unidade.

Um domínio integral é dito um *domínio de fatoração única* (DFU) se toda não unidade $a \in D$ pode ser escrita de maneira única (a menos de associados ou ordem) como um produto de elementos irredutíveis.

Exemplo 12.16

(*a*) O anel $\mathbf{Z}$ dos inteiros é o exemplo clássico de domínio de fatoração única. As unidades de $\mathbf{Z}$ são 1 e –1. Os únicos associados de $n \in \mathbf{Z}$ são n e $-n$. Os elementos irredutíveis de $\mathbf{Z}$ são números primos.

(*b*) O conjunto $D = \{a + b\sqrt{13} : a, b \text{ inteiros}\}$ é um domínio integral. As unidades de D são ± 1, $18 \pm 5\sqrt{13}$ e $-18 \pm 5\sqrt{13}$. Os elementos $2, 3 - \sqrt{13}$ e $-3 - \sqrt{13}$ são irredutíveis em D. Observe que

$$4 = 2 \cdot 2 = (3 - \sqrt{13})(-3 - \sqrt{13})$$

Portanto, D não é um domínio de fatoração única.

12.7 POLINÔMIOS SOBRE UM CORPO

Esta seção investiga polinômios cujos coeficientes pertencem a algum domínio integral ou corpo K. Em particular, mostramos que polinômios sobre um corpo K têm muitas das propriedades dos inteiros.

Definições Básicas

Seja K um domínio integral ou um corpo. Formalmente, um *polinômio f sobre K* é uma seqüência infinita de elementos de K na qual apenas um número finito de elementos é diferente de zero; isto é,

$$f = (\ldots, 0, a_n, \ldots, a_1, a_0) \qquad \text{ou equivalentemente} \qquad f(t) = a_n t^n + \cdots + a_0$$

onde o símbolo t é usado para representar um valor não determinado. Um elemento a_k é chamado *k-ésimo coeficiente* de f. Se n é o maior inteiro para o qual $a_n \neq 0$, dizemos que o *grau de f* é n; escreve-se $\deg(f) = n$[†]. Também chamamos a_n de *coeficiente pivô*[††] de f e, se $a_n = 1$, dizemos que f é um polinômio *mônico*. Por outro lado, se todo coeficiente de f é zero, então f é dito o *polinômio zero*; escreve-se $f = 0$. O grau do polinômio zero não é definido.

Seja $K[t]$ a coleção de todos os polinômios $f(t)$ sobre K. Adição e multiplicação são definidas em $K[t]$ como a seguir. Suponha que

$$f(t) = a_n t^n + \cdots + a_0 \qquad \text{e} \qquad g(t) = b_m t^m + \cdots + b_0$$

A *soma* $f + g$ é obtida pela adição dos coeficientes correspondentes; isto é, se $m \leq n$, então

$$f(t) + g(t) = a_n t^n + \cdots + (a_m + b_m)t^m + \cdots + (a_1 + b_1)t + (a_0 + b_0)$$

Além disso, o produto de f e g é o polinômio

$$f(t)g(t) = (a_n b_m)t^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)t + (a_0 b_0)$$

Isto é,

$$f(t)g(t) = c_{n+m}t^{n+m} + \cdots + c_1 t + c_0 \qquad \text{onde} \qquad c_k = \sum_{i=0}^{k} a_i b_{k-1} = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$$

O conjunto K de *escalares* é entendido como um subconjunto de $K[t]$. Especificamente, identificamos o escalar $a_0 \in K$ com o polinômio

$$f(t) = a_0 \qquad \text{ou} \qquad a_0 = (\ldots, 0, 0, a_0)$$

As operações de adição e multiplicação por escalar são preservadas por esta identificação; isto é,

$$(\ldots, 0, a_0) + (\ldots, 0, b_0) = (\ldots, 0, a_0 + b_0) \qquad \text{e} \qquad (\ldots, 0, a_0) \cdot (\ldots, 0, a_0 b_0) = (\ldots, 0, a_0 b_0)$$

Logo, a função ψ: $K \to K[t]$ definida por $\Psi(a_0) = a_0$ é um homomorfismo que insere K em $K[t]$.

Teorema 12-12: seja K um domínio integral. Então $K[t]$, munido das operações de adição e multiplicação de polinômios, é um anel comutativo com elemento identidade 1.

[†] N. de T. Do inglês, *degree*. Mantivemos a abreviatura, como em textos clássicos de álgebra em português.

[††] N. de T. No original, *leading*.

O seguinte resultado simples tem conseqüências importantes.

Lema 12.13: suponha que f e g são polinômios sobre um domínio integral K. Então,

$$\deg(fg) = \deg(f) + \deg(g)$$

A demonstração segue diretamente da definição do produto de polinômios. Isto é, suponha $f(t) = a_n t^n + \cdots + a_0$ e $g(t) = b_m t^m + \cdots + b_0$, onde $a_n \neq 0$ e $b_m \neq 0$. Então,

$$f(t)g(t) = a_n b_m t^{m+n} + \text{ termos de ordem mais baixa}$$

Além disso, como K é um domínio integral sem divisores de zero, $a_n b_m \neq 0$. Logo,

$$\deg(fg) = m + n = \deg(f) + \deg(g)$$

e a demonstração está completa.

A seguinte proposição lista muitas propriedades de polinômios. [Lembre que um polinômio g *divide* um polinômio f se existe um polinômio h tal que $f(t) = g(t)h(t)$.]

Proposição 12.14: seja K um domínio integral e sejam f e g polinômios sobre K.

(i) $K[t]$ é um domínio integral.
(ii) As unidades de $K[t]$ são as unidades de K.
(iii) Se g divide f, então, $\deg(g) \leq \deg(f)$ ou $f \equiv 0$.
(iv) Se g divide f e f divide g, então $f(t) = kg(t)$ onde k é uma unidade em K.
(v) Se d e d' são polinômios mônicos tais que d divide d' e d' divide d, então $d = d'$.

Algoritmo de Euclides, Raízes de Polinômios

Esta subseção discute as raízes de um polinômio $f(t)$ onde agora se supõe que os coeficientes de $f(t)$ pertencem a um corpo K. Lembre que um escalar $a \in K$ é uma *raiz* de um polinômio $f(t)$ se $f(a) = 0$. Começamos com um importante teorema, que é muito parecido com um teorema correspondente para os inteiros $\mathbf{Z}$.

Teorema 12-15: **(Algoritmo de divisão de Euclides)** sejam $f(t)$ e $g(t)$ polinômios sobre um corpo K com $g(t) \neq 0$. Então existem polinômios $q(t)$ e $r(t)$ tais que

$$f(t) = q(t)g(t) + r(t)$$

onde ou $r(t) \equiv 0$ ou $\deg(r) < \deg(g)$.

O teorema acima (provado no Problema 12.39) formaliza o processo conhecido como "divisão longa". O polinômio $q(t)$ é dito o *quociente*, e o polinômio $r(t)$ é dito o *resto* da divisão de $f(t)$ por $g(t)$.

Corolário 12-16: **(Teorema do resto)** suponha que $f(t)$ é dividido por $g(t) = t - a$. Então $f(a)$ é o resto.

A demonstração segue do algoritmo de Euclides. Isto é, dividindo $f(t)$ por $t - a$, temos

$$f(t) = q(t)(t - a) + r(t)$$

onde $\deg(r) < \deg(t - a) = 1$. Logo, $r(t) = r$ é um escalar. Substituindo $t = a$ na equação de $f(t)$, obtem-se

$$f(a) = q(a)(a - a) + r = q(t) \cdot 0 + r = r$$

Portanto, $f(a)$ é o resto, como afirmado.

O Corolário 12.16 também diz que $f(a) = 0$ se e somente se o resto $r = r(t) \equiv 0$. Conseqüentemente,

Corolário 12-17: **(Teorema da fatoração)** o escalar $a \in K$ é uma raiz de $f(t)$ se e somente se $t - a$ é um fator de $f(t)$.

O próximo teorema nos diz o número possível de raízes de um polinômio.

Teorema 12-18: suponha que $f(t)$ é um polinômio sobre um corpo K, e $\deg(f) = n$. Então, $f(t)$ tem no máximo n raízes.

O teorema seguinte é a ferramenta principal para determinar raízes racionais de polinômios com coeficientes inteiros.

Teorema 12-19: suponha que um número racional p/q (na forma irredutível) é raiz de um polinômio

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

onde todos os coeficientes $a_n, \ldots, a_1, a_0$ são inteiros. Então, p divide o termo constante a_0, e q divide o termo pivô a_n. Em particular, se $c = p/q$ é um inteiro, então c divide o termo constante a_0.

Exemplo 12.17

(*a*) Suponha que $f(t) = t^3 + t^2 - 8t + 4$. Assumindo que $f(t)$ tem uma raiz racional, ache todas as raízes de $f(t)$.

Como o coeficiente pivô é 1, as raízes racionais de $f(t)$ devem estar entre os inteiros $\pm 1, \pm 2, \pm 4$. Note que $f(1) \neq 0$ e $f(-1) \neq 0$. Pela divisão sintética, ou dividindo por $t - 2$, temos

$$\begin{array}{r|rrrrr} 2 & 1 & + 1 & - 8 & + 4 \\ & & 2 & + 6 & - 4 \\ \hline & 1 & + 3 & - 2 & + 0 \end{array}$$

Portanto, $t = 2$ é uma raiz de $f(t) = (t - 2)(t^2 + 3t - 2)$. Usando a fórmula quadrática para $t^2 + 3t - 2 = 0$, obtemos as seguintes raízes para $f(t)$:

$$t = 2, \qquad t = (-3 + \sqrt{17})/2, \qquad t = (-3 - \sqrt{17})/2$$

(*b*) Suponha que $h(t) = t^4 - 2t^3 + 11t - 10$. Ache as raízes reais de $h(t)$ assumindo que duas das raízes são inteiras.

As raízes inteiras estão entre $\pm 1, \pm 2, \pm 5, \pm 10$. Pela divisão sintética, ou dividindo por $t - 1$ e depois por $t + 2$, temos

$$\begin{array}{r|rrrrrr} 1 & 1 & - 2 & + 0 & + 11 & - 10 \\ & & 1 & - 1 & - 1 & + 10 \\ \hline -2 & 1 & - 1 & - 1 & + 10 & + 0 \\ & & - 2 & + 6 & - 10 & \\ \hline & 1 & - 3 & + 5 & + 0 & \end{array}$$

Logo, $t = 1$ e $t = -2$ são raízes de $h(t) = (t - 1)(t + 2)(t^2 - 3t + 5)$. A fórmula quadrática usada em $t^2 - 3t + 5$ nos conta que não existem outras raízes reais. Isto é, $t = 1$ e $t = -2$ são as únicas raízes reais de $h(t)$.

K[t] como DIP e DFU

O seguintes teoremas podem ser usados.

Teorema 12-20: o anel de polinômios sobre um corpo K, $K[t]$, é um domínio ideal principal (DIP). Se J é um ideal em $K[t]$, então existe um único polinômio mônico d que gera J, isto é, todo polinômio f em J é um múltiplo de d.

Teorema 12-21: sejam f e g polinômios em $K[t]$, e suponha que pelo menos um deles não é zero. Então existe um único polinômio mônico d tal que:

(i) d divide ambos, f e g.

(ii) Se d' divide f e g, então d' divide d.

O polinômio d no teorema acima é dito o *máximo divisor comum* de f e g e é denotado por $d = \text{mdc}(f,g)$. Se $g = 1$, f e g são ditos *primos relativos*.

Corolário 12-22: seja d o máximo divisor comum de f e g. Então, existem polinômios m e n tais que $d = mf + ng$. Em particular, se f e g são primos relativos, existem polinômios m e n tais que $mf + ng = 1$.

Um polinômio $p \in K[t]$ é dito irredutível se p não é um escalar e se $p = fg$ implica que f é um escalar ou g é um escalar. Em outras palavras, p é irredutível se seus únicos divisores são múltiplos escalares.

Lema 12.23: suponha que $p \in K[t]$ é irredutível. Se p divide o produto fg de polinômios f e g em $K[t]$, então p divide f ou p divide g. Mais genericamente, se p divide o produto $f_1 f_2 \cdots f_n$ de n polinômios, então p divide um deles.

O próximo teorema afirma que os polinômios sobre um corpo formam um domínio de fatoração única (DFU).

Teorema 12-24: **(Teorema da fatoração única)** seja f um polinômio não nulo em $K[t]$. Então f pode ser escrito de maneira única (exceto pela ordem) como um produto

$$f = kp_1p_2 \cdots p_n$$

onde $k \in K$ e os p são polinômios mônicos irredutíveis em $K[t]$.

Teorema Fundamental da Álgebra

A demonstração do teorema seguinte está além dos objetivos deste texto.

Teorema fundamental da álgebra: todo polinômio não nulo $f(t)$ sobre o corpo dos complexos **C** tem uma raiz em C. Assim, $f(t)$ pode ser escrito de maneira única (exceto pela ordem) como um produto

$$f(t) = k(t - r_1)(t - r_2) \cdots (t - r_n)$$

onde k e r_i são números complexos e $\deg(f) = n$.

O teorema acima certamente não é verdade para o corpo dos reais **R**. Por exemplo, $f(t) = t^2 + 1$ é um polinômio sobre **R**, mas $f(t)$ não tem raiz real.

O seguinte teorema pode ser usado.

Teorema 12-25: suponha que $f(t)$ é um polinômio sobre o corpo dos reais **R**, e suponha que o número complexo $z = a + bi$, $b \neq 0$, é uma raiz de $f(t)$. Então, o conjugado complexo $\bar{z} = a - bi$ também é uma raiz de $f(t)$. Portanto,

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

é um fator de $f(t)$.

Teorema 12-26: seja $f(t)$ um polinômio não nulo sobre o corpo dos reais **R**. Então, $f(t)$ pode ser escrito de maneira única (exceto pela ordem) como um produto

$$f(t) = kp_1(t)p_2(t) \cdots p_m(t)$$

onde $k \in \mathbf{R}$ e os $p_i(t)$ são polinômios reais mônicos de grau 1 ou 2.

Exemplo 12.18 Seja $f(t) = t^4 - 3t^3 + 6t^2 + 25t - 39$. Ache todas as raízes de $f(t)$ sabendo que $t = 2 + 3i$ é uma raiz.

Como $2 + 3i$ é uma raiz, $2 - 3i$ é uma raiz, e $c(t) = t^2 - 4t + 13$ é um fator de $f(t)$. Dividindo $f(t)$ por $c(t)$, obtemos

$$f(t) = (t^2 - 4t + 13)(t^2 + t - 3)$$

A fórmula quadrática em $t^2 + t - 3$ nos dá as outras raízes de $f(t)$. Isto é, as quatro raízes de $f(t)$ são:

$$t = 2 + 3i, \qquad t = 2 - 3i, \qquad t = (-1 + \sqrt{13})/2, \qquad t = (-1 - \sqrt{13})/2$$

Problemas Resolvidos

Operações e Semigrupos

12.1 Considere o conjunto **N** dos inteiros positivos, e denote por * a operação de cálculo do mínimo múltiplo comum (mmc) em **N**.

(*a*) Ache $4 * 6$, $3 * 5$, $9 * 18$ e $1 * 6$.

(*b*) (**N**, *) é um semigrupo? É comutativo?

(*c*) Ache o elemento identidade de *.

(*d*) Quais elementos em **N**, se houver, possuem inversos, e quais são esses inversos?

(*a*) Como $x * y$ significa o mínimo múltiplo comum de x e y, temos

$$4 * 6 = 12, \qquad 3 * 5 = 15, \qquad 9 * 18 = 18, \qquad 1 * 6 = 6$$

(*b*) Pode-se provar, na teoria dos números, que $(a * b) * c = a * (b * c)$, i. e., a operação de calcular o mínimo múltiplo comum é associativa, e que $a * b = b * a$, i.e., a operação é comutativa. Portanto, (**N**, *) é um semigrupo comutativo.

(*c*) O inteiro 1 é o elemento identidade já que mmc $(1, a) = a$ para todo inteiro positivo a, i.e., $1 * a = a * 1 = a$ para todo $a \in \mathbf{N}$.

(*d*) Como mmc $(a, b) = 1$ se e somente se $a = 1$ e $b = 1$, o único número com inverso é 1 e ele é o seu próprio inverso.

12.2 Considere o conjunto **Q** dos números racionais, e seja * a operação em **Q** definida por

$$a * b = a + b - ab$$

(*a*) Ache $3 * 4$, $2 * (-5)$ e $7 * \frac{1}{2}$.

(*b*) (**Q**, *) é um semigrupo? É comutativo?

(*c*) Ache o elemento identidade para *.

(*d*) Algum elemento de **Q** tem inverso? Qual?

(*a*) $3 * 4 = 3 + 4 - 3 \cdot (4) = 3 + 4 - 12 = -5.$

$2 * (-5) = 2 + (-5) - 2 \cdot (-5) = 2 - 5 + 10 = 7.$

$7 * \frac{1}{2} = 7 + \frac{1}{2} - 7(\frac{1}{2}) = 4.$

(*b*) Temos:

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc\end{aligned}$$

Portanto, * é associativa e (**Q**, *) é um semigrupo. Além disso,

$$a * b = a + b - ab = b + a - ba = b * a$$

Logo, (**Q**, *) é um semigrupo comutativo.

(*c*) Um elemento e é um elemento identidade se $a * e = a$ para todo $a \in \mathbf{Q}$. Proceda como a seguir:

$$a * e = a, \qquad a + e - ae = a, \qquad e - ea = 0, \qquad e(1 - a) = 0, \qquad e = 0$$

Conseqüentemente, 0 é o elemento identidade.

(*d*) Para que e tenha um inverso x, devemos ter $a * x = 0$ já que 0 é o elemento identidade pela parte (*c*). Proceda como a seguir:

$$a * x = 0, \qquad a + x - ax = 0, \qquad a = ax - x, \qquad a = x(a - 1), \qquad x = a/(a - 1)$$

Logo, se $a \neq 1$, então a tem inverso igual a $a/(a-1)$.

12.3 Seja S um semigrupo com identidade e, e sejam b e b' inversos de a. Mostre que $b = b'$, isto é, o inverso, se existir, é único.

Temos:

$$b * (a * b') = b * e = b \qquad \text{e} \qquad (b * a) * b' = e * b' = b'$$

Como S é associativo, $(a * b) * b' = b * (a * b')$; logo, $b = b'$.

12.4 Verifique se cada um dos seis subconjuntos de inteiros positivos $\mathbf{N}$ é fechado sob a operação de multiplicação:

(*a*) $A = \{0, 1\}$ (*d*) $D = \{2, 4, 6, \ldots\} = \{x: x \text{ é par}\}$

(*b*) $B = \{1, 2\}$ (*e*) $E = \{1, 3, 5, \ldots\} = \{x: x \text{ é ímpar}\}$

(*c*) $C = \{x: x \text{ é primo}\}$ (*f*) $F = \{2, 4, 8, \ldots\} = x: x = 2^n, n \in \mathbf{N}\}$

Dentre os seis conjuntos, quais, se algum, são fechados sob a operação de adição?

(*a*) Temos:

$$0 \cdot 0 = 0, \qquad 0 \cdot 1 = 0, \qquad 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1$$

Logo, A é fechado sob multiplicação.

(*b*) Como $2 \cdot 2 = 4$, que não pertence a B, o conjunto B não é fechado sob multiplicação.

(*c*) Note que 2 e 3 são primos, mas $2 \cdot 3 = 6$ não é; portanto, C não é fechado sob a multiplicação.

(*d*) O produto de números pares é par; logo, D é fechado sob multiplicação.

(*e*) O produto de números ímpares é ímpar; portanto, E é fechado sob multiplicação.

(*f*) Como $2^r \cdot 2^s = 2^{r+s}$, F é fechado sob multiplicação.

Como a soma de dois inteiros pares é par, o conjunto D é fechado sob adição. Entretanto, cada um dos outros conjuntos não é, pois, por exemplo,

$$1 + 1 = 2 \notin A, \qquad 3 + 5 = 8 \notin C, \qquad 2 + 4 = 6 \notin F$$
$$1 + 2 = 3 \notin B, \qquad 1 + 3 = 4 \notin E$$

12.5 Seja $S = \mathbf{N} \times \mathbf{N}$. Seja $*$ a operação em S definida por $(a, b) * (a', b') = (aa', bb')$.

(*a*) Mostre que $*$ é associativa. (Portanto, S é um semigrupo).

(*b*) Defina f: $(S, *) \to (\mathbf{Q}, \times)$ por $f(a, b) = a/b$. Mostre que f é um homomorfismo.

(*c*) Ache a relação de congruência $\sim$ em S determinada pelo homomorfismo inteiro, i.e., $x \sim y$ se $f(x) = f(y)$. (Veja o Teorema 12.4.)

(*d*) Descreva $S/\sim$. $S/\sim$ tem um elemento identidade? Tem inversos?

(*a*) Temos

$$(xy)z = (ac, bd) * (e, f) = [(ac)e, (bd)f]$$
$$x(yz) = (a, b) * (ce, df) = [a(ce), b(df)]$$

Como a, b, c, d, e e f são inteiros positivos, $(ac)e = a(ce)$ e $(bd)f = b(df)$. Logo, $(xy)z = x(yz)$ e, portanto, $*$ é associativa. Isto é, $(S, *)$ é um semigrupo.

(*b*) Temos

$$f(x * y) = f(ac, bd) = (ac)/(bd) = (a/b)(c/d) = f(x)f(y)$$

Logo, f é um homomorfismo.

(*c*) Suponha que $f(x) = f(y)$. Então,

$$\frac{a}{b} = \frac{c}{d} \text{ e, portanto, } ad = bc.$$

Logo, f determina a relação de congruência $\sim$ em S definida por $(a, b) \sim (c, d)$ se $ad = bc$.

(*d*) A imagem de f é $\mathbf{Q}^*$, o conjunto dos números racionais positivos. Pelo Teorema 12.3, $S/\sim$ é isomorfo a $\mathbf{Q}^*$. Logo, $S/\sim$ tem um elemento identidade, e todo elemento tem um inverso.

12.6 Seja $S = \mathbf{N} \times \mathbf{N}$. Seja $*$ a operação em S definida por

$$(a, b) * (a', b') = (a + a', b + b')$$

(*a*) Mostre que $*$ é associativa. (Portanto, S é um semigrupo.)

(*b*) Defina $f: (S, *) \to (\mathbf{Z}, +)$ por $f(a, b) = a - b$. Mostre que f é um homomorfismo.

(*c*) Ache a relação de congruência $\sim$ em S determinada pelo homomorfismo f, i.e., $x \sim y$ se $f(x) = f(y)$. (Veja o Teorema 12.4.)

(*d*) Descreva $S/\sim$. $S/\sim$ tem elemento identidade? Tem inversos?

Suponha $x = (a, b)$, $y = (c, d)$ e $z = (e, f)$.

(*a*) Temos

$$(xy)z = (a + c, b + d) * (e, f) = [(a + c) + e, (b + d) + f]$$
$$x(yz) = (a, b) * (c + e, d + f) = [a + (c + e), b + (d + f)]$$

Como a, b, c, d, e e f são inteiros positivos,

$$(a + c) + e = a + (c + e) \qquad \text{e} \qquad (b + d) + f = b + (d + f)$$

Logo, $(xy)z = x(yz)$ e, portanto, $*$ é associativa. Isto é, $(S, *)$ é um semigrupo.

(*b*) Temos

$$f(x * y) = f(a + c, b + d) = (a + c) - (b + d) = (a - b) + (c - d) = f(x)f(y)$$

Portanto, f é um homomorfismo.

(*c*) Suponha que $f(x) = f(x)$. Então $a - b = c - d$ e, portanto, $a + d = b + c$. Logo, f determina a relação de congruência $\sim$ em S definida por:

$$(a, b) \sim (c, d) \text{ se } a + d = b + c$$

(*d*) A imagem de f é todo o conjunto $\mathbf{Z}$ já que todo inteiro é a diferença de dois inteiros positivos. Portanto, pelo Teorema 12.3, $S/\sim$ é isomorfo a $\mathbf{Z}$. Logo, $S/\sim$ tem um elemento identidade, e todo elemento tem inverso (aditivo).

12.7 Prove o Teorema 12.1: suponha que $*$ é uma operação associativa em um conjunto S. Então, todo produto $a_1 * a_2 * \cdots * a_n$ prescinde de parênteses, isto é, todas as possibilidades são iguais.

A demonstração é por indução sobre n. Como $*$ <None>é associativa, o teorema vale para $n = 1$, 2 e 3. Suponha que $n \geq 4$. Usaremos a notação:

$$(a_1a_2, \cdots a_n) = (\cdots((a_1a_2)a_3)\cdots)a_n \qquad \text{e} \qquad [a_1a_2\cdots a_n] = \text{ qualquer produto}$$

Mostramos que $[a_1a_2\cdots a_n] = (a_1a_2\cdots a_n)$, o que implica que todos os produtos deste tipo são iguais. Como $[a_1a_2\cdots a_n]$ denota algum produto, existe um $r < n$ tal que $[a_1a_2\cdots a_n] = [a_1a_2\cdots a_r][a_{r+1}\cdots a_n]$. Portanto, por indução,

$$\begin{aligned}[a_1a_2\cdots a_n] &= [a_1a_2\cdots a_r][a_{r+1}\cdots a_n] = [a_1a_2\cdots a_r](a_{r+1}\cdots a_n)\\ &= [a_1\cdots a_r]((a_{r+1}\cdots a_{n-1})a_n) = ([a_1\cdots a_r](a_{r-1}\cdots a_{n-1}))a_n\\ &= [a_1\cdots a_{n-1}]a_n = (a_1\cdots a_{n-1})a_n = (a_1a_2\cdots a_n)\end{aligned}$$

Assim, o teorema fica demonstrado.

12.8 Prove o Teorema 12.4: seja $f: S \to S'$ um homomorfismo de semigrupos. Defina $a \sim b$ se $f(a) = f(b)$. Então: (i) $\sim$ é uma relação de congruência, (ii) $S/\sim$ é isomorfo a $f(S)$.

(i) Mostramos primeiramente que $\sim$ é uma relação de equivalência. Como $f(a) = f(a)$, $a \sim a$. Se $a \sim b$, então $f(a) = f(b)$ ou $f(b) = f(a)$ e, portanto, $b \sim a$. Finalmente, se $a \sim b$ e $b \sim c$, então $f(a) = f(b)$ e $f(b) = f(c)$ e, portanto, $f(a) = f(c)$. Logo, $a \sim c$. Isto é, $\sim$ é uma relação de equivalência. Suponha agora que $a \sim a'$ e $b \sim b'$. Então, $f(a) = f(a')$ e $f(b) = f(b')$. Como f é um homomorfismo,

$$f(ab) = f(a)f(b) = f(a')f(b') = f(a'b')$$

Portanto, $ab \sim a'b'$. Isto é, $\sim$ é uma relação de congruência.

Hidden page

Hidden page

12.12 Sejam σ e τ os seguintes elementos do grupo simétrico S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \qquad \text{e} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$$

Ache $\tau\sigma$, $\sigma\tau$, σ^2 e σ^{-1}. (Como τ e σ são funções, $\tau\sigma$ significa aplicar σ e depois τ.)

O efeito de σ e depois τ em 1, 2, ..., 6 está representado na Figura 12-8(*a*). O efeito de τ e depois σ em 1, 2, ..., 6 está representado na Figura 12-8(*b*); o efeito de σ e depois σ novamente em 1, 2, ..., 6 está representado na Figura 12-8(*c*). Logo,

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix} \qquad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix} \qquad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$$

Obtemos σ^{-1} trocando as linhas inferior e superior de σ e rearranjando:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 6 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$$

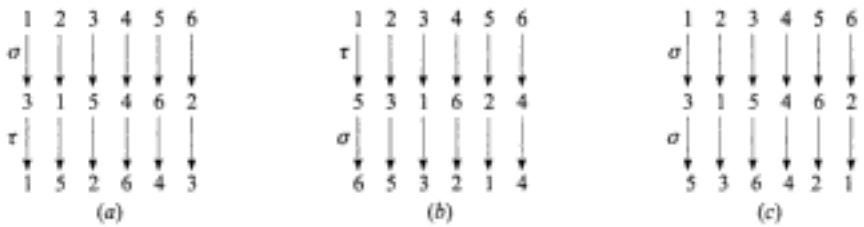


Fig. 12-8

12.13 Seja S o quadrado no plano $\mathbf{R}^2$ desenhado na Figura 12-9, com o ponto central na origem 0. Note que os vértices de S estão numerados no sentido anti-horário de 1 para 4. (*a*) Defina o grupo G de simetria de S. (*b*) Liste os elementos de G. (*c*) Ache um conjunto de geradores mínimo para G.

(*a*) Uma simetria σ de S é uma correspondência rígida injetora de S em si mesmo. (Aqui, rígido significa que a distância entre dois pontos não muda.) O grupo G de simetrias de S é o conjunto de todas as simetrias de S sob a composição de funções.

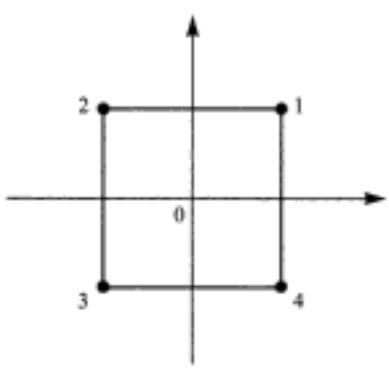


Fig. 12-9

(*b*) Existem oito simetrias, como descrito a seguir. Para $\alpha = 0°$, $90°$, $180°$ e $270°$, seja $\sigma(\alpha)$ a simetria obtida pela rotação de S de α graus em torno da origem e seja $\tau(\alpha)$ a simetria obtida pela reflexão de S no eixo y, seguida de rotação de α graus em torno da origem. Observe que qualquer simetria de S é determinada pelo seu efeito nos vértices de S e, portanto, σ pode ser representada como uma permutação em S_4. Logo,

$$\sigma(0^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \sigma(90^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \sigma(180^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$
$$\sigma(270^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$
$$\tau(0^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \tau(90^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \tau(180^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$
$$\tau(270^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(*c*) Sejam $a = \sigma(90^\circ)$ e $b = \tau(0^\circ)$. Então a e b formam um conjunto mínimo de geradores de G. Especificamente,

$$\sigma(0^\circ) = a^4, \quad \sigma(90^\circ) = a, \quad \sigma(180^\circ) = a^2, \quad \sigma(270^\circ) = a^3$$
$$\tau(0^\circ) = b, \quad \tau(90^\circ) = ba, \quad \tau(180^\circ) = ba^2, \quad \tau(270^\circ) = ba^3$$

e G não é cíclico não sendo gerado por um elemento. (É possível mostrar que as relações $a^4 = e$, $b^2 = e$ e $bab = a^{-1}$ descrevem G completamente.)

12.14 Sejam H e K grupos. (*a*) Defina o produto direto $G = H \times K$ de H e K. (*b*) Qual é o elemento identidade de $G = H \times K$? (*c*) Descreva e exiba a tabela de multiplicação para o grupo $G = \mathbf{Z}_2 \times \mathbf{Z}_2$.

(*a*) Seja $G = H \times K$ o produto cartesiano de H e K com a operação $*$ definida componente a componente por

$$(h, k) * (h'k') = (hh', kk')$$

Então, G é um grupo (Problema 12.73) denominado o *produto direto* de H e K.

(*b*) O elemento $e = (e_H, e_K)$ é o elemento identidade de G, e $|G| = |H||K|$.

(*c*) Como $\mathbf{Z}_2$ tem dois elementos, G tem quatro elementos. Sejam

$$e = (0, 0), \quad a = (1, 0), \quad b = (0, 1), \quad c = (1, 1)$$

A tabela de multiplicação de G está na Figura 12-10. Note que G é abeliano, uma vez que sua tabela é simétrica. Também

$$a^2 = e, \quad b^2 = e, \quad c^2 = e$$

Assim, G não é cíclico e, portanto, $G \not\approx \mathbf{Z}_4$.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Fig. 12-10

12.15 Seja G um grupo e seja A um conjunto não vazio.

(*a*) Defina o sentido da frase "G age em A".

(*b*) Defina o estabilizador H_a de um elemento $a \in A$.

(*c*) Mostre que H_a é um subgrupo de G.

(*a*) Seja PERM(A) o grupo de todas as permutações de A. Defina ψ: $G \to$ PERM(A) um homomorfismo qualquer. Dizemos, então, que G *age em* A e cada elemento de G define uma permutação g: $A \to A$ por:

$$g(a) = (\Psi(g))(a)$$

(Freqüentemente, a permutação g: $A \to A$ é dada diretamente e, portanto, o homomorfismo ψ é definido implicitamente.)

Hidden page

Hidden page

Hidden page

(*a*) Pelo Problema 12.83, os inteiros relativamente primos ao *modulus* $m = 10$ são as unidades de $\mathbf{Z}_{10}$. Portanto, as unidades são 1, 3, 7 e 9.

(*b*) Em um anel R, $-a$ significa o elemento tal que $a + (-a) = 0$. Portanto, $-3 = 7$, já que $3 + 7 = 7 + 3 = 0$ em $\mathbf{Z}_{10}$. Analogamente, $-8 = 2$, e a^{-1} em um anel R é o elemento tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Portanto, $3^{-1} = 7$, já que $3 \cdot 7 = 7 \cdot 3 = 1$ em $\mathbf{Z}_{10}$.

(*c*) Substitua cada elemento de $\mathbf{Z}_{10}$ em $f(x)$ para verificar quais deles tornam $f(x)$ igual a 0. Temos

$$\begin{array}{lllll} f(0) = 4, & f(2) = 0, & f(4) = 2, & f(6) = 0, & f(8) = 4 \\ f(1) = 0, & f(3) = 4, & f(5) = 4, & f(7) = 0, & f(9) = 2 \end{array}$$

Logo, as raízes são 1, 2, 6 e 7. (Este exemplo mostra que um polinômio de grau n pode ter mais de n raízes sobre um anel arbitrário. Isto não ocorre se o anel for um corpo).

12.29 Prove que, em um anel R, (i) $a \cdot 0 = 0 \cdot a = 0$; (ii) $a(-b) = (-a)b = -ab$; (iii) $(-1)a = -a$ (quando R tem o elemento 1).

(i) Como $0 = 0 + 0$, temos

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ a ambos os lados, obtemos $0 = a \cdot 0$. Analogamente, $0 \cdot a = 0$.

(ii) Usando $b + (-b) = (-b) + b = 0$, temos

$$ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$$
$$a(-b) + ab = a((-b) + b) = a \cdot 0 = 0$$

Portanto, $a(-b)$ é o negativo de ab; isto é, $a(-b) = -ab$. Analogamente, $(-a)b = -ab$.

(iii) Temos

$$a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$$
$$(-1)a + a = (-1)a + 1 \cdot a = ((-1) + 1)a = 0 \cdot a = 0$$

Portanto, $(-1)a$ é o negativo de a; isto é, $(-1)a = -a$.

12.30 Em um domínio integral D, mostre que, se $ab = ac$ com $a \neq 0$, então, $b = c$.

Como $ab = ac$, temos

$$ab - ac = 0 \qquad \text{e, portanto,} \qquad a(b - c) = 0$$

Como $a \neq 0$, devemos ter $b - c = 0$, já que D não tem divisores de zero. Logo, $b = c$.

12.31 Suponha que J e K sejam ideais em um anel R. Mostre que $J \cap K$ é um ideal em R.

Como J e K são ideais, $0 \in J$ e $0 \in K$. Portanto, $0 \in J \cap K$. Agora, considere $a, b \in J \cap K$ e seja $r \in R$. Então, $a, b \in J$ e $a, b \in K$. Como J e K são ideais,

$$a - b,\ ra,\ ar \in J \qquad \text{e} \qquad a - b,\ ra,\ ar \in K$$

Logo, $a - b$, ra, $ar \in J \cap K$. Assim, $J \cap K$ é um ideal.

12.32 Seja J um ideal em um anel R com elemento identidade 1. Prove: (*a*) Se $1 \in J$, então $J = R$. (*b*) Se qualquer unidade $u \in J$, então $J = R$.

(*a*) Se $1 \in J$, então para todo $r \in R$, temos $r \cdot 1 \in J$ ou $r \in J$. Portanto, $J = R$.

(*b*) Se $u \in J$, então u^{-1} ou $1 \in J$. Logo, $J = R$ pela parte (*a*).

12.33 Prove: (*a*) Um domínio integral finito D é um corpo.
(*b*) $\mathbf{Z}_p$ é um corpo, onde p é um número primo.
(*c*) (Fermat) Se p é um primo, então $a^p \equiv a \pmod{p}$ para todo inteiro a.

(*a*) Suponha que D tem n elementos, digamos $D = \{a_1, a_2, \ldots, a_n\}$. Seja a qualquer elemento não nulo de D. Considere os elementos

$$aa_1, \quad aa_2, \quad \ldots, \quad aa_n$$

Como $a \neq 0$, temos que $aa_i = aa_j$ implica $a_i = a_j$ (Problema 12.30). Logo, os n elementos acima são distintos e, portanto, devem ser uma reordenação dos elementos de D; isto é, $aa_k = 1$. Logo, a_k é o inverso de a. Como a é um elemento não nulo qualquer de D, concluímos que D é um corpo.

(*b*) Lembre que $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$. Mostraremos que $\mathbf{Z}_p$ não tem divisores de zero. Suponha que $a * b = 0$ em $\mathbf{Z}_p$; isto é, $ab \equiv 0 (\text{mod } p)$. Então, p divide ab. Como p é um primo, p divide a ou p divide b. Portanto, $a \equiv 0 (\text{mod } p)$ ou $b \equiv 0 (\text{mod } p)$; isto é, $a = 0$ ou $b = 0$ em $\mathbf{Z}_p$. Conseqüentemente, $\mathbf{Z}_p$ não tem divisores de zero e, portanto, $\mathbf{Z}_p$ é um domínio integral. Pela parte (*a*), $\mathbf{Z}_p$ é um corpo.

(*c*) Se p divide a, então $a \equiv 0 (\text{mod } p)$ e, assim, $a^p \equiv a \equiv 0 \pmod p$. Suponha que p não divide a. Então a pode ser visto como um elemento não nulo em $\mathbf{Z}_p$. Como $\mathbf{Z}_p$ é um corpo, seus elementos não nulos formam um grupo G sob multiplicação de ordem $p-1$. Pelo Problema 12.21, $a^{p-1} = 1$ em $\mathbf{Z}_p$. Em outras palavras, $a^{p-1} \equiv 1 \pmod p$. Multiplicando por a, obtém-se $a^p \equiv a \pmod p$, e o teorema fica demonstrado.

Polinômios sobre um Corpo

12.34 Suponha que $f(t) = t^3 - 2t^2 - 6t - 3$. Ache as raízes de $f(t)$ sabendo que $f(t)$ tem uma raiz inteira.

As raízes inteiras de $f(t)$ devem ser ± 1 ou ± 3. Note que $f(1) \neq 0$. Usando a divisão sintética ou dividindo por $t - 1$, obtemos

$$\begin{array}{r|rrrr} -1 & 1 & -2 & -6 & -3 \\ & & -1 & +3 & +3 \\ \hline & 1 & -3 & -3 & +0 \end{array}$$

Portanto, $t = -1$ é uma raiz de $f(t)$. Podemos usar agora a fórmula quadrática em $t^2 - 3t - 3$ para obter as três raízes seguintes de $f(t)$:

$$t = -1, \qquad t = (3 + \sqrt{21})/2, \qquad t = (3 - \sqrt{21})/2$$

12.35 Suponha que $f(t) = 2t^3 - 3t^2 - 6t - 2$. Ache todas as raízes de $f(t)$ sabendo que $f(t)$ tem uma raiz racional.

As raízes racionais de $f(t)$ só podem ser $\pm 1, \pm 2$ ou $\pm \frac{1}{2}$. Testando cada possibilidade para raiz, obtemos, usando divisão sintética (ou dividindo por $2t + 1$),

$$\begin{array}{r|rrrr} -\frac{1}{2} & 2 & -3 & -6 & -2 \\ & & -1 & +2 & +2 \\ \hline & 2 & -4 & -4 & +0 \end{array}$$

Portanto, $t = -\frac{1}{2}$ é uma raiz e

$$f(t) = (t + \tfrac{1}{2})(2t^2 - 4t - 4) = (2t + 1)(t^2 - 2t - 2)$$

Podemos agora usar a forma quadrática em $t^2 - 2t - 2$ para obter as seguintes três raízes de $f(t)$:

$$t = -\tfrac{1}{2}, \qquad t = 1 + \sqrt{3}, \qquad t = 1 - \sqrt{3}$$

12.36 Seja $f(t) = t^4 - 3t^3 + 3t^2 + 3t - 20$. Ache todas as raízes de $f(t)$ sabendo que $t = 1 + 2i$ é uma raiz.

Como $1 + 2i$ é uma raiz, $1 - 2i$ é raiz, e $c(t) = t^2 - 2t + 5$ é fator de $f(t)$. Dividindo $f(t)$ por $c(t)$, obtemos

$$f(t) = (t^2 - 2t + 5)(t^2 - t - 4)$$

A fórmula quadrática com $t^2 - t - 4$ nos dá as outras raízes de $f(t)$. Isto é, as quatro raízes de $f(t)$ são

$$t = 1 + 2i, \qquad t = 1 - 2i, \qquad t = (1 + \sqrt{17})/2, \qquad t = (1 - \sqrt{17})/2$$

12.37 Seja $K = \mathbf{Z}_8$. Ache todas as raízes de $f(t) = t^2 + 6t$.

Aqui, $\mathbf{Z}_8 = \{0, 1, 2, \ldots, 7\}$. Substituindo cada elemento de $\mathbf{Z}_8$ em $f(t)$, obtemos

$$f(0) = 0, \qquad f(2) = 0, \qquad f(4) = 0, \qquad f(6) = 0$$

Então, $f(t)$ tem quatro raízes, $t = 0, 2, 4, 6$. (O Teorema 12.21 não pode ser usado, já que K não é um corpo.)

12.38 Suponha que $f(t)$ é um polinômio real de grau n ímpar.

(*a*) Mostre algebricamente que $f(t)$ tem uma raiz real.

(*b*) Mostre geometricamente que $f(t)$ tem uma raiz real.

(*a*) As raízes complexas de $f(t)$ ocorrem aos pares. Como $f(t)$ tem um número ímpar de raízes (contando a multiplicidade), $f(t)$ precisa ter pelo menos uma raiz real.

(*b*) Suponha que o coeficiente pivô de $f(t)$ seja positivo [se não for, multiplique $f(t)$ por -1]. Como o grau de $f = n$, com n ímpar, temos

$$\lim_{t\to\infty} f(t) = +\infty \qquad \text{e} \qquad \lim_{t\to-\infty} f(t) = -\infty$$

Logo, o gráfico de $f(t)$ precisa cortar o eixo t em pelo menos um ponto, como mostrado na Figura 12-11.

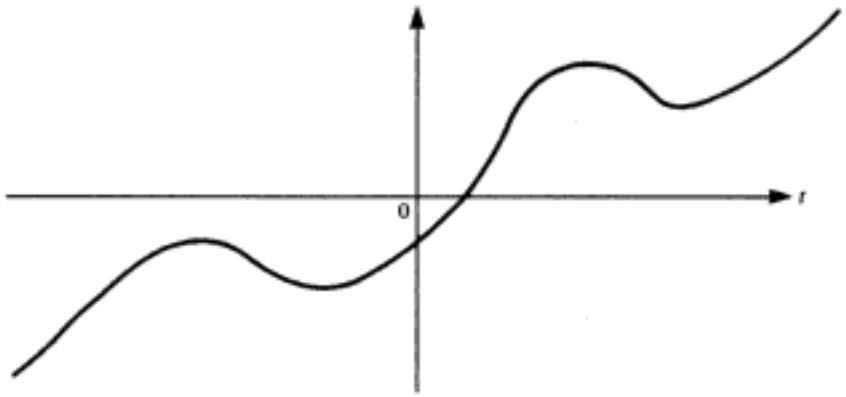


Fig. 12-11

12.39 Prove o Teorema 12.15 (algoritmo de divisão de Euclides): sejam $f(t)$ e $g(t)$ polinômios sobre um corpo K com $g(t) \neq 0$. Então, existem polinômios $q(t)$ e $r(t)$ tais que

$$f(t) = q(t)g(t) + r(t)$$

onde ou $r(t) \equiv 0$ ou $\deg(r) < \deg(g)$.

Se $f(t) = 0$ ou $\deg(f) < \deg(g)$, então temos a representação desejada $f(t) = 0g(t) + f(t)$. Agora, suponha que $\deg(f) \geq \deg(g)$, digamos $f(t) = a_n t^n + \cdots + a_1 t + a_0$ e $g(t) = b_m t^m + \cdots + b_1 t + b_0$, onde $a_n, b_m \neq 0$ e $n \geq m$. Formamos o polinômio

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t) \qquad (1)$$

(Este é o primeiro passo na subtração no algoritmo de "divisão longa".) Então, $\deg(f_1) < \deg(f)$. Por indução, existem polinômios $q_1(t)$ e $r(t)$ tais que $f_1(t) = q_1(t)g(t) + r(t)$, onde ou $r(t) \equiv 0$ ou $\deg(r) < \deg(g)$. Substituindo em (1) e resolvendo para $f(t)$, obtemos

$$f(t) = \left(q_1(t) + \frac{a_n}{b_m} t^{n-m}\right) g(t) + r(t)$$

que é a representação desejada.

12.40 Prove o Teorema 12.18: suponha que $f(t)$ é um polinômio sobre um corpo K e $\deg(f) = n$. Então, $f(t)$ tem, no máximo, n raízes.

A prova é feita por indução sobre n. Se $n = 1$, então $f(t) = at + b$ e $f(t)$ tem a raiz única $t = -b/a$. Suponha que $n > 1$. Se $f(t)$ não tem raízes, então o teorema é verdade. Suponha que $a \in K$ seja raiz de $f(t)$. Então,

$$f(t) = (t - a)g(t) \qquad (1)$$

onde $\deg(g) = n - 1$. Afirmamos que qualquer outra raiz de $f(t)$ também é raiz de $g(t)$. Suponha que $b \neq a$ também é raiz de $f(t)$. Substituindo $t = b$ em (1), temos $0 = f(b) = (b - a)g(b)$. Como K não tem divisores de zero e $b - a \neq 0$, devemos ter $g(b) = 0$. Por indução, $g(t)$ tem, no máximo, $n - 1$ raízes. Logo, $f(t)$ tem, no máximo, $n - 1$ raízes além de a. Portanto, $f(t)$ tem no máximo n raízes.

12.41 Prove o Teorema 12.19: suponha que o número racional p/q (na forma irredutível) é raiz do polinômio

$$f(t) = a_n t^n + \cdots + a_1 t + a_0$$

onde os coeficientes $a_n, \ldots, a_1, a_0$ são inteiros. Então, p divide o termo constante a_0, e q divide o coeficiente pivô a_n. Em particular, se $c = p/q$ é um inteiro, então c divide o termo constante a_0.

Substitua o termo $t = p/q$ em $f(t) = 0$ para obter $a_n(p/q)^n + \cdots + a_1(p/q) + a_0 = 0$. Multiplique ambos os lados da equação por q^n para obter

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0 \qquad (1)$$

Como p divide todos os primeiros n termos de (1), p deve dividir o último termo $a_0 q^n$. Admitindo que p e q são primos relativos, p divide a_0. Analogamente, q divide os últimos n termos de (1); logo, q divide o primeiro termo $a_n p^n$. Como p e q são primos relativos, q divide a_n.

12.42 Prove o Teorema 12.20: o anel $K[t]$ de polinômios sobre um corpo K é um domínio ideal principal (DIP). Se J é um ideal em $K[t]$, então existe um único polinômio mônico d que gera J, isto é, todo polinômio f em J é um múltiplo de d.

Seja d um polinômio de grau mínimo em J. Como podemos multiplicar d por um escalar não nulo permanecendo em J, assumimos, sem perda de generalidade, que d é um polinômio mônico. Suponha agora que $f \in J$. Pelo algoritmo de divisão, existem polinômios q e r tais que $f = qd + r$ onde $r = 0$ ou $\deg(r) < \deg(d)$. Mas $f, d \in J$ implica que $qd \in J$ e, portanto, $r = f - qd \in J$. Mas d é um polinômio de grau mínimo em J. Conseqüentemente, $r = 0$ ou $f = qd$, isto é, d divide f. Resta mostrar que d é único. Se d' for outro polinômio mônico que gera J, então d divide d' e d' divide d. Isto implica que $d = d'$, porque d e d' são mônicos. Assim, o teorema está provado.

12.43 Prove o Teorema 12.21: sejam f e g polinômios em $K[t]$, sem que ambos sejam o polinômio zero. Então, existe um único polinômio mônico tal que: (i) d divide ambos, f e g; (ii) se d' divide f e g, então d' divide d.

O conjunto $I = \{mf + ng, n \in K[t]\}$ é um ideal. Seja d o polinômio mônico que gera I. Note que $f, g \in I$; logo, d divide f e g. Agora suponha que d' divide f e g. Seja J o ideal gerado por d'. Então, $f, g \in J$ e, portanto, $I \subseteq J$. Conseqüentemente, $d \in J$ e logo d' divide d como afirmado anteriormente. Resta mostrar que d é único. Se d_1 for outro máximo divisor comum (mônico) de f e g, então d divide d_1 e d_1 divide d. Isto implica $d = d_1$, porque d e d_1 são mônicos. Assim, o teorema está provado.

12.44 Prove o Corolário 12.22: seja d o máximo divisor comum de f e g. Então, existem polinômios m e n tais que $d = mf + ng$. Em particular, se f e g são relativamente primos, então existem polinômios m e n tais que $mf + ng = 1$.

Da demonstração do Teorema 12.21 no Problema 12.43, o máximo divisor comum d gera o ideal $I = \{mf + ng : m, n \in K[t]\}$. Logo, existem polinômios m e n tais que $d = mf + ng$.

12.45 Prove o Lema 12.23: suponha que $p \in K[t]$ é irredutível. Se p divide o produto fg de polinômios $f, g \in K[t]$, então p divide f ou p divide g. Mais genericamente, se p divide o produto $f_1 f_2 \cdots f_n$ de n polinômios, então p divide algum deles.

Suponha que p divide fg mas não f. Como p é irredutível, os polinômios f e p devem ser relativamente primos. Portanto, existem polinômios m e $n \in K[t]$ tais que $mf + np = 1$. Multiplicando esta equação por g, obtemos $mfg + npg = g$. Mas p divide fg e, portanto, p divide mfg e p divide npg. Logo, p divide a soma $g = mfg + npg$.

Agora suponha que p divide $f_1 f_2 \cdots f_n$. Se p divide f_1, o lema está provado. Senão, pelo resultado acima, p divide o produto $f_2 \cdots f_n$. Por indução sobre n, p divide um dos polinômios $f_2, \cdots, f_n$, e o lema está provado.

12.46 Prove o Teorema 12.24 (teorema da fatoração única): seja f um polinômio não nulo em $K[t]$. Então, f pode ser escrito de maneira única (exceto pela ordem) como um produto $f = kp_1 p_2 \cdots p_n$ onde $k \in K$ e os ps são polinômios mônicos irredutíveis em $K[t]$.

Mostraremos primeiramente a existência de um tal produto. Se f é irredutível ou, se $f \in K$, o produto claramente existe. Por outro lado, suponha que $f = gh$ onde g e h não são escalares. Então, g e h têm grau menor do que o grau de f. Por indução, podemos assumir que $g = k_1 g_1 g_2 \cdots g_r$ e $h = k_2 h_1 h_2 \cdots h_s$, onde $k_1, k_2 \in K$ e os g_i e h_j são polinômios mônicos irredutíveis. Conseqüentemente $f = (k_1 k_2) g_1 g_2 \cdots g_r h_1 h_2 \cdots h_s$ é a representação desejada.

Provaremos agora a unicidade (exceto pela ordem) de um tal produto para f. Suponha que

$$f = kp_1p_1 \cdots p_n = k'q_1q_2 \cdots q_m \qquad \text{onde} \qquad k, k' \in K$$

e que $p_1, \cdots, p_n, q_1, \cdots, q_m$ são polinômios irredutíveis mônicos. Agora, p_1 divide $k'q_1 \cdots q_m$. Como p_1 é irredutível ele deve dividir pelo menos um dos qs pelo Lema 12.23. Suponha que p_1 divide q_1. Como p_1 e q_1 são ambos irredutíveis e mônicos, $p_1 = q_1$. Conseqüentemente, $kp_2 \cdots p_n = k'q_2 \cdots q_m$. Por indução, temos que $n = m$ e $p_2 = q_2, \cdots, p_n = q_m$ para alguma reordenação dos q_i. Também temos que $k = k'$. Assim, o teorema fica provado.

12.47 Prove o Teorema 12.25: suponha que $f(t)$ é um polinômio sobre o corpo dos reais $\mathbf{R}$, e suponha que o número complexo $z = a + bi$, $b \neq 0$, é uma raiz de $f(t)$. Então, o complexo conjugado também é uma raiz de $f(t)$. Portanto,

$$c(t) = (t - z)(t - \bar{z}) = t^2 - 2at + a^2 + b^2$$

é um fator de $f(t)$.

Como grau$(c) = 2$, existem $q(t)$ e números reais M e N tais que

$$f(t) = c(t)q(t) + Mt + N \tag{1}$$

Como $z = a + bi$ é uma raiz de $f(t)$ e $c(t)$, temos, substituindo $t = a + bi$ em (1),

$$f(z) = c(z)q(z) + M(z) + n \qquad \text{ou} \qquad 0 = 0q(z) + M(z) + N \qquad \text{ou} \qquad M(a + bi) + N = 0$$

Logo, $Ma + N = 0$ e $Mb = 0$. Como $b \neq 0$, concluímos que $M = 0$. Portanto, $0 + N = 0$ ou $N = 0$. Conseqüentemente, $f(t) = c(t)q(t)$ e $\bar{z} = a - bi$ é uma raiz de $f(t)$.

Problemas Complementares

Operações e Semigrupos

12.48 Seja $*$ a operação no conjunto dos números reais $\mathbf{R}$ definida por $a * b = a + b + 2ab$.

(*a*) Ache $2 * 3$, $3 * (-5)$ e $7 * (1/2)$

(*b*) $(\mathbf{R}, *)$ é um semigrupo? É comutativo?

(*c*) Ache o elemento identidade.

(*d*) Que elementos têm inversos e quais são os inversos?

12.49 Seja A um conjunto não vazio com a operação $*$ definida como $a * b = a$, e assuma que A tem mais de um elemento. (*a*) A é um semigrupo? (*b*) A é comutativo? (*c*) A tem elemento identidade? (*d*) Quais elementos (se algum) têm inverso e quais são os inversos?

12.50 Seja $A = \{a, b\}$. Ache o número de operações em A e exiba uma que não seja nem associativa nem comutativa.

12.51 Seja $A = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$, i.e., os múltiplos de 3. A é fechado sob (*a*) adição, (*b*) multiplicação, (*c*) subtração, (*d*) divisão (exceto por 0)?

12.52 Ache um conjunto A de três números que seja fechado sob (*a*) adição, (*b*) multiplicação.

12.53 Seja S um conjunto infinito. Seja A a coleção de subconjuntos finitos de S e seja B a coleção de subconjuntos infinitos de S.

(*a*) A é fechado sob (i) união; (ii) interseção, (iii) complementares?

(*b*) B é fechado sob (i) união; (ii) interseção, (iii) complementares?

12.54 Seja $S = \mathbf{Q} \times \mathbf{Q}$ o conjunto de pares ordenados de números racionais, com a operação $*$ definida por

$$(a, b) * (x, y) = (ax, ay + b)$$

(*a*) Ache $(3, 4) * (1, 2)$ e $(-1, 3) * (5, 2)$.

(*b*) S é um semigrupo? É comutativo?

(*c*) Ache o elemento identidade de S.

(*d*) Quais elementos (se algum) têm inversos e quais são os inversos?

Hidden page

12.67 Seja H um subgrupo de G com apenas duas classes laterais. Mostre que H é normal.

12.68 Seja S um polígono regular com n lados, e seja G o grupo de simetrias de S. (*a*) Ache a ordem de G. (*b*) Mostre que G é gerado por dois elementos a e b tais que $a^n = e$, $b^2 = e$ e $b^{-1}ab = a^{-1}$. (G é chamado de *grupo diedral*.)

12.69 Suponha que um grupo G age em um conjunto S por um homomorfismo $\psi: G \to \text{PERM}(S)$.

(*a*) Prove que, para todo $s \in S$: (i) $e(s) = s$, e (ii)$(gg')(s) = g(g'(s))$ onde $g, g' \in G$.

(*b*) A *órbita* de G, para qualquer $s \in S$, é definida por $G_s = \{g(s): g \in G\}$. Mostre que as órbitas formam uma partição de S.

(*c*) Mostre que $|G_s| = [G: H_s]$, o número de classes laterais dos estabilizadores H_s de s em G. [Lembre que $H_s = \{g \in G: g(s) = s\}$.]

12.70 Seja G um grupo abeliano e seja n um inteiro positivo fixo. Mostre que a função $f: G \to G$ definida por $f(a) = a^n$ é um homomorfismo.

12.71 Seja G um grupo multiplicativo de números complexos z tais que $|z| = 1$, e seja $\mathbf{R}$ o grupo aditivo de números reais. Prove que $G \simeq \mathbf{R}/\mathbf{Z}$.

12.72 Suponha que H e N são subgrupos de G com N normal. Mostre que (*a*)HN é subgrupo de G; (*b*) $H \cap N$ é um subgrupo normal de H; (*c*) $H/(H \cap N) \simeq HN/N$.

12.73 Sejam H e K grupos. Seja G o conjunto produto $H \times K$ com a operação

$$(h, k) * (h', k') = (hh', kk')$$

(*a*) Mostre que G é um grupo (chamado de *produto direto* de H e K.)

(*b*) Seja $H' = H \times \{e\}$. Mostre que: (i) $H' \cong H$; (ii) H' é um subgrupo normal de G; (iii) $G/H' \cong K$.

Anéis

12.74 Considere o anel $\mathbf{Z}_{12} = \{0, 1, \ldots, 11\}$ dos inteiros módulo 12. Ache (*a*) as unidades de $\mathbf{Z}_{12}$; (*b*) as raízes de $f(x) = x^2 + 4x + 4$ sobre $\mathbf{Z}_{12}$; (*c*) os associados de 2.

12.75 Considere o anel $\mathbf{Z}_{30} = \{0, 1, \ldots, 29\}$ dos inteiros módulo 30. Ache (*a*) $-2, -7, -11$; (*b*) 7^{-1}, 11^{-1} e 26^{-1}.

12.76 Mostre que, em um anel R, (*a*) $(-a)(-b) = ab$; (*b*) $(-1)(-1) = 1$, se R tiver o elemento identidade 1.

12.77 Suponha que $a^2 = a$ para todo $a \in R$. (Um anel com essa propriedade é chamado *anel booleano*.) Prove que R é comutativo.

12.78 Seja R um anel com elemento identidade 1. Transformamos R em um novo anel R' definindo

$$a \oplus b = a + b + 1 \qquad \text{e} \qquad a * b = ab + a + b$$

(*a*) Verifique que R' é um anel. (*b*) Determine os elementos 0 e 1 de R'.

12.79 Seja G um grupo abeliano (aditivo) qualquer. Defina uma multiplicação em G por $a \cdot b = 0$ para todo $a, b \in G$. Mostre que isto transforma G em um anel.

12.80 Sejam J e K ideais em um anel R. Prove que $J + K$ e $J \cap K$ também são ideais.

12.81 Seja R um anel com elemento identidade. Mostre que $(a) = \{ra: r \in R\}$ é o menor ideal contendo a.

12.82 Mostre que R e $\{0\}$ são ideais de qualquer anel R.

12.83 Prove que (*a*) as unidades de um anel R formam um grupo sob multiplicação. (*b*) as unidades em $\mathbf{Z}_m$ são os inteiros primos relativos de m.

12.84 Para todo inteiro positivo m, verifique que $m\mathbf{Z} = \{rm: r \in \mathbf{Z}\}$ é um anel. Mostre que $2\mathbf{Z}$ e $3\mathbf{Z}$ não são isomorfos.

12.85 Prove o Teorema 12.10: seja J um ideal em um anel R. Então, as classes laterais $\{a + J: a \in R\}$ formam um anel sob as operações nas classes laterais

$$(a + J) + (b + J) = a + b + J \qquad \text{e} \qquad (a + J)(b + J) = ab + J$$

12.86 Prove o teorema 12.11: seja $f: R \to R'$ um homomorfismo de anéis com *kernel* K. Então, K é um ideal em R, e o quociente R/K é isomorfo a $f(R)$.

12.87 Seja J um ideal em um anel R. Considere o mapeamento canônico $f: R \to R/J$ definido por $f(a) = a + J$. Mostre que: (a) f é um homomorfismo de anéis; (b) f é um mapeamento sobrejetor.

12.88 Suponha que J é um ideal em um anel R. Mostre que:

(a) Se R é comutativo, R/J é comutativo.

(b) Se R tem elemento unidade 1 e se $1 \notin J$, então $1 + R$ é um elemento unidade para R/J.

Domínios Integrais e Corpos

12.89 Prove que, se $x^2 = 1$ é um domínio integral D, então $x = -1$ ou $x = 1$.

12.90 Seja $R \neq \{0\}$ um anel comutativo finito sem divisores de zero. Mostre que R é um domínio integral, i.e., que R tem um elemento identidade 1.

12.91 Prove que $F = \{a + b\sqrt{2}: a, b \text{ racionais}\}$ é um corpo.

12.92 Prove que $F = \{a + b\sqrt{2}: a, b \text{ inteiros}\}$ é um domínio integral mas não um corpo.

12.93 Um número complexo $a + bi$ onde a, b são inteiros é chamado de *inteiro gaussiano*. Mostre que o conjunto G dos *inteiros gaussianos* é um domínio integral. Mostre também que as unidades são ± 1 e $\pm i$.

12.94 Seja R um domínio integral e seja J um ideal em R. Prove que o anel quociente R/J é um domínio integral se e somente se J é um ideal primo. (Um ideal J *é primo* se $J \neq r$ e se $ab \in J$ implica $a \in J$ ou $b \in J$.)

12.95 Seja R um anel comutativo com elemento identidade 1, e seja J um ideal em R. Prove que o anel R/J é um corpo se e somente se J é um ideal maximal. (Um ideal J é *maximal* se $J \neq R$ e nenhum ideal K estiver estritamente contido entre J e R, isto é, se $J \subseteq K \subseteq R$, então $J = K$ ou $K = R$.)

12.96 Seja D um ideal de matrizes reais 2×2 da forma $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Mostre que D é isomorfo ao corpo dos complexos $\mathbf{C}$; portanto, D é um corpo.

12.97 Mostre que os únicos ideais em um corpo K são $\{0\}$ e o próprio K.

12.98 Suponha que $f: K \to K'$ é um homomorfismo de um corpo K em um corpo K'. Mostre que f é uma *imersão*; isto é, f é injetora. [Assumimos que $f(1) = 0$)].

12.99 Considere o domínio integral $D = \{a + b\sqrt{13}: a, b \text{ inteiros}\}$. [Veja o Exemplo 12.16(*b*)]. Se $\alpha = a + b\sqrt{13}$, definimos $N(\alpha) = a^2 - 13b^2$. Mostre: (i) $N(\alpha\beta) = N(\alpha)N(\beta)$. (ii) α é uma unidade se e somente se $N(\alpha) = \pm 1$. (iii) Dentre as unidades de D, estão ± 1, $18 \pm 5\sqrt{13}$ e $18 \pm 5\sqrt{13}$. (iv) Os números 2, $3 - \sqrt{13}$ e $3 - \sqrt{13}$ são irredutíveis.

Polinômios sobre um Corpo

12.100 Ache as raízes de $f(t)$ assumindo que $f(t)$ tem uma raiz inteira.
(a) $f(t) = t^3 - t^2 - 11t - 10$; (b) $f(t) = t^3 + 2t^2 - 13t - 6$.

12.101 Ache as raízes de $f(t)$ assumindo que $f(t)$ tem uma raiz racional. (a) $f(t) = 2t^3 - 3t^2 - 16t - 7$;
(b) $f(t) = 2t^3 - t^2 - 9t + 9$.

12.102 Ache as raízes de $f(t) = t^4 - 5t^3 + 16t^2 - 9t - 13$, sabendo que $t = 2 + 3i$ é uma raiz.

12.103 Ache as raízes de $f(t) = t^4 - t^3 - 5t^2 + 12t - 10$, sabendo que $t = 1 - i$ é uma raiz.

12.104 Para um escalar qualquer $a \in K$, defina a *função avaliação* $\psi_a: K[t] \to K$ por $\psi_a(f(t)) = f(a)$. Mostre que ψ_a é um homomorfismo de anéis.

12.105 Prove a Proposição 12.14.

12.106 Prove o Teorema 12.26

Respostas dos Problemas Complementares

12.48 (*a*) 17, –32, 29/2, (*b*) sim, sim; (*c*) zero; (*d*) se $a \neq 1/2$, então a tem um inverso que é $-a/(1+2a)$.

12.49 (*a*) Sim; (*b*) não; (*c*) não; (*d*) não tem sentido falar em inversos quando não existe elemento identidade.

12.50 São 16, já que existem duas escolhas, a ou b, para cada um dos quatro produtos aa, ab, ba e bb. Na Figura 12-12, $ab \neq ba$. Além disso, $(aa)b = bb = a$, mas $a(ab) = aa = b$.

*	a	b
a	b	a
b	b	a

Fig. 12-12

12.51 (*a*) Sim; (*b*) sim; (*c*) sim; (*d*) não.

12.52 (*a*) $\{1, -1, 0\}$; (*b*) não existe qualquer conjunto.

12.53 (*a*) Sim, sim, não; (*b*) sim, não, não.

12.54 (*a*) (3, 10), (–5, 1); (*b*) sim, não; (*c*) (1, 0); (*d*) o elemento (a, b) tem um inverso $a \neq 0$, e seu inverso $(1/a, -b/a)$.

12.55 (*a*) (19, 20), (18/7). (*b*) Sim. (*d*) $(a, b) \sim (c, d)$ se $ad = bc$. (*e*) $S/\sim$ é isomorfo aos números racionais positivos sob adição. Logo, $S/\sim$ não tem elemento identidade nem inversos.

12.56 (*a*) $H = \{0, 5, 10, 15\}$ e $|H| = 3$.

(*b*) H, $1 + H = \{1, 6, 11, 16\}$, $2 + H = \{2, 7, 12, 17\}$, $3 + H = \{3, 8, 13, 18\}$, $4 + H = \{4, 9, 14, 19\}$.

12.57 (*a*) Veja a Figura 12-13.

(*b*) $5^{-1} = 11$, $7^{-1} = 13$, $17^{-1} = 17$.

(*c*) (i) $gp(5) = G$, $|5| = 6$; (ii) $gp(13) = \{1, 7, 13\}$, $|13| = 3$.

(*d*) Sim, pois $G = gp(5)$.

×	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Fig. 12-13

12.58 (*a*) $|1| = 1$, $|5| = 2$, $|7| = 2$, $|11| = 2$; (*b*) não; (*c*) $G, \{1\}, \{1, 7\}, \{1, 5\}, \{1, 11\}$

Hidden page

Capítulo 13

Linguagens, Gramáticas e Máquinas

13.1 INTRODUÇÃO

Pode-se olhar um computador como uma máquina M que tem as propriedades descritas a seguir. A cada instante, M tem um "estado interno", M lê alguma "entrada", M "imprime" alguma saída que depende apenas do estado interno e da entrada e, então, possivelmente, M muda o estado interno. Existem várias maneiras de formalizar a noção de uma máquina M bem como uma hierarquia de tais máquinas.

Pode-se também definir uma função "computável" em termos de um tipo especial de máquina M (máquina de Turing) que produz uma saída inteira não negativa $M(n)$ para qualquer entrada inteira não negativa n. Como a maioria dos dados pode ser codificada por tais inteiros, a máquina M pode tratar a maior parte dos dados.

Este capítulo é dedicado a essas questões e a tópicos a elas relacionados.

13.2 ALFABETOS, PALAVRAS E SEMIGRUPOS LIVRES

Considere um conjunto não vazio A de símbolos. Uma *palavra* ou *string* w no conjunto A é uma seqüência finita de elementos do alfabeto. Por exemplo, as seqüências

$$u = ababb \qquad \text{e} \qquad v = accbaaa$$

são palavras em $A = \{a, b, c\}$. Quando tratamos de palavras em A, freqüentemente denominamos A como o *alfabeto*, e seus elementos são chamados de *letras*. Também usaremos notação abreviada escrevendo a^2 para aa, a^3 para aaa e assim por diante. Logo, para as palavras acima, $u = abab^2$ e $v = ac^2ba^3$.

A seqüência vazia, denotada por λ (letra grega lambda), ε (letra grega épsilon) ou 1, também é considerada uma palavra em A, chamada de *palavra vazia*. O conjunto de todas as palavras em A é denotado por A^*.

O *comprimento* de uma palavra u (escreve-se $|u|$ ou $l(u)$) é o número de elementos na sua seqüência de letras. Para as palavras u e v acima, temos $l(u) = 5$ e $l(v) = 7$. Além disso, $l(\lambda) = 0$, onde λ é a palavra vazia.

Observação: A menos que afirmação em contrário seja feita, o alfabeto A será finito, os símbolos u, v e w estarão reservados para palavras em A e os elementos de A usarão as letras a, b e c.

Concatenação

Considere duas palavras u e v em um alfabeto A. A *concatenação* de u e v, denotada por uv, é a palavra obtida quando se escrevem as letras de u seguidas das letra de v. Por exemplo, para as palavra u e v acima, temos

$$uv = ababbaccbaaa = abab^2ac^2ba^3$$

A exemplo das letras, definimos $u^2 = uu$, $u^3 = uuu$ e, em geral, $u^{n+1} = uu^n$, onde u é uma palavra.

Claramente, para quaisquer palavras u, v e w, as palavras $(uv)w$ e $u(vw)$ são idênticas, consistindo, simplesmente, nas letras u, v e w escritas uma após a outra. Também, o acoplamento da palavra vazia antes ou depois de qualquer palavra u não altera a palavra u. Em outros termos:

Teorema 13-1: a operação de concatenação de palavras em um alfabeto A é associativa. A palavra vazia λ é o elemento identidade da operação.

(Falando em termos gerais, a operação não é comutativa, por exemplo, $uv \neq vu$ para as palavras u e v acima.)

Subpalavras e Segmentos Iniciais

Considere qualquer palavra $u = a_1a_2 \cdots a_n$ em um alfabeto A. Qualquer seqüência $w = a_ja_{j+1} \cdots a_k$ é chamada *subpalavra* de u. Em particular, a subpalavra $w = a_1a_2 \cdots a_k$, começando com as primeiras letras de u, é dita um *segmento inicial* de u. Em outros termos, w é uma subpalavra de u se $u = v_1wv_2$, e w é um segmento inicial de u se $u = wv$. Observe que λ e u são subpalavras de u, já que $u = \lambda u$.

Considere a palavra $u = abca$. As subpalavras e segmentos iniciais de u são:

(1) Subpalavras: λ, a, b, c, ab, bc, ca, abc, bca, $abca$.
(2) Segmentos iniciais: λ, a, ab, abc, $abca$.

Observe que a subpalavra $w = a$ aparece em dois lugares de u. A palavra ac não é uma subpalavra de u mesmo que todas as letras pertençam a u.

Semigrupos Livres e Monóides Livres

Seja F o conjunto de palavras não vazias de um alfabeto A com a operação de concatenação. Como observado acima, a operação é associativa. Assim F é um semigrupo, chamado *semigrupo livre sobre A* ou *semigrupo livre gerado por A*. Pode-se mostrar facilmente que F satisfaz as leis de cancelamento à direita e à esquerda. Entretanto, F não é comutativo quando A tem mais de um elemento. Escreveremos F_A para o semigrupo livre sobre A quando quisermos especificar o conjunto A.

Considere agora $M = A^*$ o conjunto de todas as palavras de A, incluindo a palavra vazia λ. Como λ é um elemento identidade para a operação de concatenação, M é um monóide, chamado *monóide livre* sobre A.

13.3 LINGUAGENS

Uma *linguagem L sobre* um conjunto A é uma coleção de palavras em A. Lembre que A^* denota o conjunto de todas as palavras em A. Portanto, a linguagem L é, simplesmente, um subconjunto de A^*.

Exemplo13.1 Os seguintes conjuntos são linguagens sobre A.

(*a*) $L_1 = \{a, ab, ab^2, \ldots\}$.
(*b*) $L_2 = \{a^mb^n : m > 0, n > 0\}$.
(*c*) $L_3 = \{a^mb^m : m > 0\}$.
(*d*) $L_4 = \{b^mab^n : m \geq 0, n \geq 0\}$.

Pode-se, verbalmente, descrever essas linguagens como a seguir.

(*a*) L_1 consiste em todas as palavras começando por a e seguidas de zero ou mais bs.
(*b*) L_2 consiste em todas as palavras começando por um ou mais a e seguidas por um ou mais bs.
(*c*) L_3 consiste em todas as palavras começando por um ou mais a e seguidas pelo mesmo número de bs.
(*d*) L_4 consiste em todas as palavras com exatamente um a.

Operações em Linguagens

Suponha que L e M são linguagens sobre um alfabeto A. A "concatenação" de L e M, denotada por LM, é a linguagem definida como a seguir:

$$LM = \{uv : u \in L, v \in M\}$$

isto é, LM denota o conjunto de todas as palavras que vêm da concatenação de uma palavra de L com uma palavra de M. Por exemplo, suponha

$$L_1 = \{a, b^2\} \qquad L_2 = \{a^2, ab, b^3\}, \qquad L_3 = \{a^2, a^4, a^6, \ldots\}$$

Então,

$$\begin{aligned} L_1L_2 &= \{a^3, a^2b, ab^3, b^2a^2, b^2ab, b^5\} \\ L_1L_3 &= \{a^3, a^5, a^7, \ldots, b^2a^2, b^2a^4, b^2a^6, \ldots\} \\ L_1L_1 &= \{a^2, ab^2, b^2a, b^4\} \end{aligned}$$

Claramente, a concatenação de linguagens é associativa, já que a concatenação de palavras é associativa.

As *potências* de uma linguagem L são definidas como a seguir.

$$L^0 = \{\lambda\}, \qquad L^1 = L, \qquad L^2 = LL, \qquad L^{m+1} = L^mL \quad \text{para} \quad m > 1.$$

A operação unária L^* (lê-se "L estrela") de uma linguagem L, conhecida como o *fecho de Kleene* de L, porque Kleene provou o Teorema 13.2, é definida como a união finita

$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots = \bigcup_{k=0}^{\infty} L^k$$

A definição de L^* é coerente com a notação A^* que consiste em todas as palavras sobre A. Alguns textos definem L^+ como sendo a união de $L^1, L^2, \ldots$, isto é, L^+ é a mesma coisa que L^*, mas sem a palavra vazia λ.

13.4 EXPRESSÕES REGULARES E LINGUAGENS REGULARES

Seja A um alfabeto (não vazio). Esta seção define uma expressão regular r sobre A e uma linguagem $L(r)$ sobre A associada à expressão regular r. A expressão r e sua linguagem correspondente $L(r)$ são indutivamente definidas a seguir.

Definição: Cada uma das expressões seguintes é uma expressão regular sobre um alfabeto A.

(1) O símbolo "λ" (palavra vazia) e o par "( )" (expressão vazia) são expressões regulares.
(2) Cada letra a em A é uma expressão regular.
(3) Se r é uma expressão regular, então (r^*) é uma expressão regular.
(4) Se r_1 e r_2 são expressões regulares, $(r_1 \vee r_2)$ é uma expressão regular.
(5) Se r_1 e r_2 são expressões regulares, então (r_1r_2) é uma expressão regular.

Todas as expressões regulares são formadas dessa maneira.

Observe que uma expressão regular r é um tipo especial de palavra (*string*) que usa as letras de A e os cinco símbolos

$$(\qquad)\qquad^*\qquad\vee\qquad\lambda$$

Enfatizamos que nenhum outro símbolo é usado em expressões regulares.

Definição: Uma linguagem $L(r)$ sobre A, definida por uma expressão regular r sobre A, é definida como:

(1) $L(\lambda) = \{\lambda\}$ e $L(\,(\,)\,) = \varnothing$, o conjunto vazio.
(2) $L(a) = \{a\}$, onde a é uma letra em A.
(3) $L(r^*) = (L(r))^*$, o fecho de Kleene $L(r)$.
(4) $L(r_1 \vee r_2) = L(r_1) \cup L(r_2)$ (a união das linguagens).
(5) $L(r_1r_2) = L(r_1)L(r_2)$ (a concatenação das linguagens).

Hidden page

Hidden page

A Linguagem *L(M)* Determinada por um Autômato *M*

Cada autômato M com um alfabeto de entrada A define uma linguagem sobre A, denotada por $L(M)$, como a seguir.

Seja $w = a_1 a_2 \cdots a_m$ uma palavra em A. Então w determina uma seqüência de estados

$$s_0 \to s_1 \to s_2 \to \cdots \to s_m$$

onde s_0 é o estado inicial e $F(s_{i-1}, a_i) = s_i$ para $i \geq 1$. Em outras palavras, w determina o caminho

$$P = (s_0, a_1, s_1, a_2, s_2, \ldots, a_m, s_m)$$

no grafo do diagrama de estados $D(M)$.

Dizemos que M *reconhece* a palavra w se o estado final s_m for um estado aceitável em Y. A linguagem de M, $L(M)$, é a coleção de todas as palavras de A que são aceitáveis por M.

Exemplo 13.5

(*a*) Determine se o autômato M na Figura 13-2 aceita ou não a palavra w onde: (1) $w = ababba$; (2) $w = baab$; (3) $w = \lambda$.

(1) Use a Figura 13-2 e a palavra $w = ababba$ para obter o caminho

$$P = s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{b} s_1 \xrightarrow{b} s_2 \xrightarrow{a} s_2$$

(2) A palavra $w = baab$ determina o caminho

$$P = s_0 \xrightarrow{b} s_1 \xrightarrow{a} s_0 \xrightarrow{a} s_0 \xrightarrow{b} s_1$$

O estado final s_1 está em Y; portanto, w é aceitável por M.

(3) Aqui o estado final é igual ao estado inicial s_0 já que w é a palavra vazia. Como s_0 está em Y, λ é aceitável por M.

(*b*) Descreva a linguagem $L(M)$ do autômato M na Figura 13-2.

$L(M)$ consistirá em todas as palavras w de A que não têm dois bs sucessivos. Isso decorre dos fatos seguintes:

(1) Podemos entrar com o estado s_2 apenas após dois bs sucessivos.

(2) Nunca podemos sair de s_2.

(3) O estado s_2 é o único estado rejeitado (não aceitável).

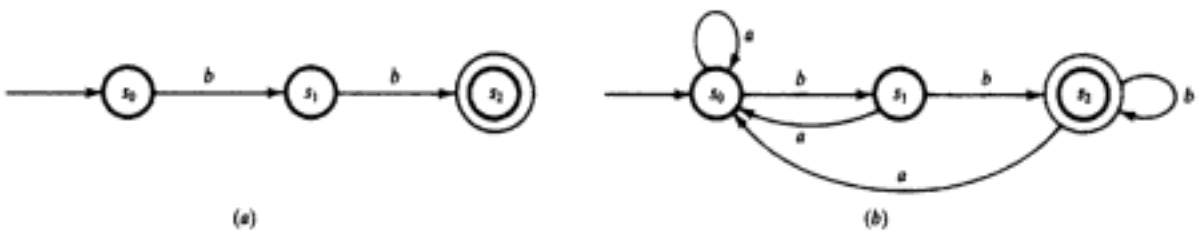
A relação fundamental entre linguagens regulares e *automata* está contida no teorema seguinte (cuja prova está além dos objetivos deste texto).

Teorema 13-2: (**Kleene**) uma linguagem L sobre um alfabeto A é regular se e somente se existe um autômato de estado finito M tal que $L = L(M)$.

A operação estrela L^* em uma linguagem L é chamada, às vezes, de fecho de Kleene de L, já que Kleene foi quem primeiramente provou este resultado básico.

Exemplo 13.6 Seja $A = \{a, b\}$. Construa um autômato M que aceitará precisamente as palavras de A que terminam com dois b.

Como b^2 é aceitável, mas λ e b não o são, precisamos de três estados, s_0, o estado inicial e s_1 e s_2 com uma seta rotulada com b indo de s_0 para s_1, e outra de s_1 para s_2. Além disso, s_2 é um estado aceitável, mas não s_0 e s_1. Isto nos dá o grafo da Figura 13-3(*a*). Por outro lado, se existe um a, então queremos voltar a s_0, e se estivermos em s_2 e existir um b, então queremos ficar em s_2. Essas condições adicionais permitem determinar o autômato desejado M que aparece na Figura 13-3(*b*).



Flig. 13-3

Hidden page

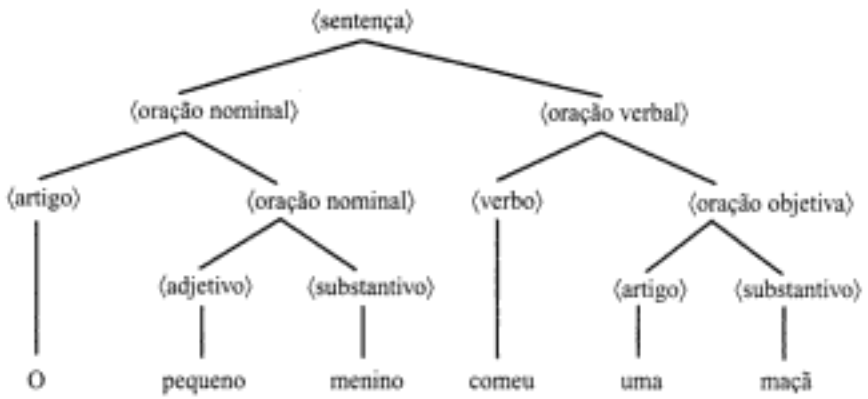


Fig. 13-5

Uma *gramática de estrutura de frases* ou, simplesmente, uma *gramática* G consiste em quatro partes:

(1) um conjunto finito (*vocabulário*) V;

(2) um subconjunto T de V cujos elementos são chamados *terminais* (os elementos de $N = V \backslash T$ são denominados *não terminais* ou *variáveis*);

(3) um símbolo não terminal S chamado símbolo de *start*[1];

(4) um conjunto finito P de produções. Uma produção é um par ordenado (α, β), normalmente denotado por $\alpha \to \beta$, onde α e β são palavras em V. Cada produção em V deve conter pelo menos uma variável no seu lado esquerdo.

Uma tal gramática G é denotada por $G = G(V, T, S, P)$ quando queremos indicar suas quatro partes.

As seguintes notações, a menos que declaração em contrário seja feita ou esteja implícita, serão usadas para a nossa gramática. Terminais serão denotados por letras minúsculas latinas em itálico, $a, b, c, \ldots$, e variáveis serão denotadas por letras latinas em itálico maiúsculas $A, B, C, \ldots$ usando S para o símbolo de *start*. Letras gregas, $\alpha, \beta, \ldots$ denotarão palavras em V, isto é, palavras envolvendo terminais e não-terminais. Além disto, escreveremos

$$\alpha \to (\beta_1, \beta_2, \ldots, \beta_k) \qquad \text{em vez de} \qquad \alpha \to \beta_1,\ \alpha \to \beta_2, \ldots,\ \alpha \to \beta_k,$$

Observação: Freqüentemente, definiremos uma palavra G apresentando apenas suas produções, assumindo implicitamente que S é o símbolo de *start* e que os terminais e não-terminais de G são apenas aqueles que aparecem em suas produções.

Exemplo 13.8 Definimos a seguir uma gramática G:

$$V = \{A, B, S, a, b\}, \qquad T = \{a, b\}, \qquad P = \{S \xrightarrow{1} AB, A \xrightarrow{2} Aa, B \xrightarrow{3} Bb, A \xrightarrow{4} a, B \xrightarrow{5} b\}$$

com S como símbolo de *start*. As produções podem ser abreviadas como a seguir.

$$S \to AB, \qquad A \to (Aa, a), \qquad B \to (Bb, b)$$

Linguagem $L(G)$ de uma Gramática G

Suponha que w e w' são palavras sobre um conjunto vocabulário V de uma gramática G. Escrevemos

$$w \Rightarrow w'$$

Se w' pode ser obtida de w usando uma das produções, isto é, se existem palavras u e v tais que $w = u\alpha v$ e $w' = u\beta v$ e existe uma produção $\alpha \to \beta$. Escrevemos

$$w \Rightarrow\Rightarrow w' \qquad \text{ou} \qquad w \overset{*}{\Rightarrow} w'$$

se w' pode ser obtida a partir de w usando um número finito de produções.

[1] N. de T. Deixamos o nome como no original dada a freqüência de seu uso sem tradução. Alguns textos utilizam o termo "símbolo incial".

Seja G uma gramática com conjunto terminal T. A linguagem de G, denotada por $L(G)$, consiste em todas as palavras em T que podem ser obtidas do símbolo de *start* S pelo processo descrito anteriormente; isto é,

$$L(G) = \{w \in T^* : S \Rightarrow\Rightarrow w\}$$

Exemplo 13.9 Considere a gramática G no Exemplo 13.8. Observe que $w = a^2b^4$ pode ser obtida do símbolo de *start* S como a seguir:

$$S \Rightarrow AB \Rightarrow AaB \Rightarrow aaB \Rightarrow aaBb \Rightarrow aaBbb \Rightarrow aaBbbb \Rightarrow aabbbb = a^2b^4$$

Aqui, usamos as produções 1, 2, 4, 3, 3, 3, 5, respectivamente. Logo, podemos escrever $S \Rightarrow\Rightarrow a^2b^4$. Portanto, $w = a^2b^4$ pertence a $L(G)$. Mais geralmente, a seqüência e produções 1, 2 (r vezes), 4, 3 (s vezes), 5 produzirá a palavra $w = a^r ab^s b$, onde r e s são inteiros não negativos. Por outro lado, nenhuma seqüência de produções pode produzir a depois de um b. Conseqüentemente,

$$L(G) = \{a^m b^n : m \text{ e } n \text{ inteiros positivos}\}$$

Isto é, a linguagem $L(G)$ da gramática G consiste em todas as palavras que começam com um ou mais as seguidos por um ou mais b.

Exemplo 13.10 Ache a linguagem $L(G)$ sobre $\{a, b, c\}$ gerada pela gramática G com produções

$$S \to aSb, \qquad aS \to Aa, \qquad Aab \to c$$

Primeiramente, precisamos aplicar a primeira produção uma ou mais vezes para obter a palavra $w = a^n Sb^n$, onde $n > 0$. Para eliminar S, aplicamos a segunda produção para obter a palavra $w' = a^m Aabb^m$, onde $m = n - 1 \geq 0$. Finalmente, só nos resta aplicar a terceira produção para obter a palavra $w'' = a^m cb^m$ onde $m \geq 0$. Conseqüentemente,

$$L(G) = \{a^m cb^m : m \text{ não negativo}\}$$

Isto é, $L(G)$ consiste em todas as palavras com o mesmo número não negativo de a e b separados por um c.

Tipos de Gramáticas

As gramáticas são classificadas de acordo com os tipos de produção possíveis. A seguinte classificação de gramáticas é devida a Noam Chomsky.

Uma gramática de Tipo 0 não tem restrições nas suas produções. Os Tipos 1, 2 e 3 são definidos como a seguir:

(1) Uma gramática G é dita ser de Tipo 1 se toda produção é da forma $\alpha \to \beta$ onde $|\alpha| \leq |\beta|$ ou da forma $\alpha \to \lambda$.

(2) Uma gramática G é dita ser de Tipo 2 se toda produção é da forma $A \to \beta$, i. é., onde o lado esquerdo é um não terminal.

(3) Uma gramática G é dita ser de Tipo 3 se toda produção é da forma $A \to a$ ou $A \to aB$, i.e., onde o lado esquerdo é uma única variável, e o lado direito é um terminal simples ou um terminal seguido de uma variável, ou da forma $S \to \lambda$.

Observe que as gramáticas formam uma hierarquia; isto é, toda gramática do Tipo 3 é uma gramática do Tipo 2, toda gramática do Tipo 2 é uma gramática do Tipo 1 e toda gramática do Tipo 1 é uma gramática do Tipo 0.

As gramáticas também são classificadas como sensíveis a contexto, livres de contexto ou regulares.

(a) Uma gramática é dita *sensível a contexto* se as produções são da forma

$$\alpha A \alpha' \to \alpha \beta \alpha'$$

A denominação "sensível a contexto" vem do fato de que podemos substituir a variável A por β em uma palavra apenas quando A estiver entre α e α'.

(b) Uma gramática G é dita *livre de contexto* se as suas produções são da forma

$$A \to \beta$$

A denominação "livre de contexto" vem do fato de que agora podemos substituir a variável A por β a despeito do local onde A aparece.

(*c*) Uma gramática é dita *regular* se as suas produções são da forma

$$A \to a, \qquad A \to aB, \qquad S \to \lambda$$

Observe que gramática livre de contexto tem o mesmo sentido que gramática do Tipo 2, e uma gramática regular é igual a uma gramática do Tipo 3.

Uma relação fundamental entre gramáticas regulares e autômatos finitos é enunciada a seguir.

Teorema 13-4: uma linguagem L pode ser gerada por uma gramática G do Tipo 3 (regular) se e somente se existe um autômato finito M que aceita L.

Portanto, a linguagem L é regular sse $L = L(r)$, onde r é uma expressão regular sse $L = L(M)$ onde M é um autômato finito sse $L = L(G)$, onde G é uma gramática regular. (Lembre que sse é a abreviatura de "se e somente se".)

Exemplo 13.11 Considere a linguagem $L = \{a^n b^n;\ n > 0\}$.

(*a*) Ache uma gramática G, livre de contexto, que gera L.

Claramente, a gramática G com as seguintes produções vai gerar L:

$$S \to ab, \qquad S \to aSb$$

Note que G é uma linguagem livre de contexto, pois cada lado esquerdo é um não terminal.

(*b*) Ache uma gramática regular G que gera L.

Pelo Exemplo 13.7, L não é uma linguagem regular. Portanto, L não pode ser gerada por uma gramática regular.

Árvores de Derivação de Gramáticas Livres de Contexto

Considere uma gramática livre de contexto G (Tipo 2). Qualquer derivação de uma palavra w em $L(G)$ pode ser representada graficamente por uma árvore com raízes ordenada T, denominada *árvore de derivação* ou *parse tree*[†]. Por exemplo, seja G a gramática livre de contexto com as seguintes produções:

$$S \to aAB, \qquad A \to Bba, \qquad B \to bB, \qquad B \to c$$

A palavra $w = acbabc$ pode ser derivada de S como a seguir:

$$S \Rightarrow aAB \to a(Bba)B \Rightarrow acbaB \Rightarrow acba(bB) \Rightarrow acbabc$$

Pode-se desenhar uma árvore de derivação T, a partir da palavra w, como indicado na Figura 13-6. Especificamente, iniciamos com S como raiz e depois adicionamos ramos à árvore de acordo com a produção usada na derivação de w. Esse procedimento leva à árvore completa mostrada na Figura 13-6(*e*). A seqüência de folhas, da esquerda para a direita, em T é a palavra derivada w. Além disso, qualquer nó que não seja uma folha em T é uma variável, digamos A, e os sucessores imediatos (filhos) de A formam uma palavra α onde $A \to \alpha$ é a produção de G usada na derivação de w.

Forma de Bakus-Naur

Existe uma outra notação, chamada de forma de Bakus-Naur, que é geralmente usada para descrever as produções de uma gramática livre de contexto (Tipo 2). Especificamente,

(i) $::=$ é usado em vez de $\to$.

(ii) Todo não-terminal aparece dentro de delimitadores $\langle\ \rangle$.

(iii) Todas as produções com os mesmos não-terminais do lado esquerdo são combinadas em uma declaração com todos os lados direitos listados à direita de $::=$, separados por barras verticais.

[†] N. de T. A tradução literal seria "árvore de análise sintática".

Por exemplo, as produções $A \to a\,B$, $A \to b$, $A \to BC$ são combinadas em uma única sentença

$$\langle A \rangle \ ::= a\langle B \rangle | b | \langle B \rangle \langle C \rangle$$

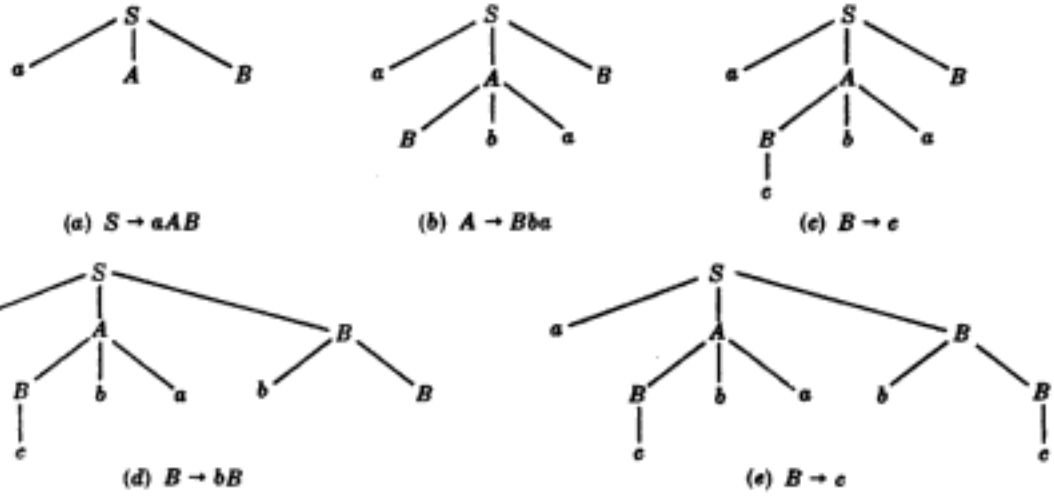


Fig. 13-6

Máquinas e Gramáticas

O Teorema 13.4 nos conta que linguagens regulares correspondem a autômatos (AEF). Também existem máquinas, mais funcionais do que AEF, que correspondem a outras gramáticas.

(*a*) ***Autômatos de pilha***: um autômato de pilha P é similar a um AEF exceto pelo fato de que P tem uma uma pilha auxiliar que torna disponível uma quantidade infinita de memória para P. Uma linguagem L é reconhecida por um autômato de pilha P se e somente se L é livre de contexto.

(*b*) ***Autômatos linearmente limitados***: um autômato linearmente limitado B dispõe de mais recursos do que um autômato de pilha. Um tal autômato B usa uma fita que é linearmente limitada pelo comprimento da palavra de entrada w. Uma linguagem L é reconhecida por um autômato linearmente limitado se e somente se L é sensível ao contexto.

(*c*) ***Máquinas de Turing***: uma máquina de Turing M, assim denominada em homenagem ao matemático britânico Alan Turing, usa uma fita infinita. Ela é capaz de reconhecer qualquer linguagem L que pode ser gerada por qualquer gramática de estrutura de frases G. Na verdade, uma máquina de Turing M é uma das muitas maneiras equivalentes de definir uma função "computável" f.

A discussão acerca de autômatos de pilha e autômatos linearmente limitados está além dos objetivos deste texto. Discutiremos máquinas de Turing na Seção 13.8.

13.7 MÁQUINAS DE ESTADO FINITO

Uma máquina de estado finito (MEF) é similar a um autômato de estado finito exceto pelo fato de que uma máquina de estado finito "imprime" uma saída usando um alfabeto de saída distinto do alfabeto de entrada. Apresentamos a seguir a definição formal.

Uma *máquina de estado finito* (ou *máquina seqüencial completa*) M consiste em seis partes:

(1) um conjunto finito A de símbolos de entrada;
(2) um conjunto finito S de "estados internos";
(3) um conjunto finito Z de símbolos de saída;
(4) um estado inicial s_0 em S;
(5) uma função de próximo estado f de $S \times A$ em S;
(6) uma função de saída g de $S \times A$ em Z.

Uma máquina como esta é denotada por $M = M(A, S, Z, s_0, f, g)$ quando se quer indicar suas seis partes.

Exemplo13.12 As informações seguintes definem uma máquina de estado finito M com dois símbolos de entrada, três estados internos e três símbolos de saída:

(1) $A = \{a, b\}$;
(2) $S = \{s_0, s_1, s_2\}$;
(3) $Z = \{x, y, z\}$;
(4) Estado inicial s_0;
(5) Função de próximo estado f: $S \times A \to S$ definida por

$$\begin{array}{lll} f(s_0, a) = s_1, & f(s_1, a) = s_2, & f(s_2, a) = s_0 \\ f(s_0, b) = s_2, & f(s_1, b) = s_1, & f(s_2, b) = s_1 \end{array}$$

(6) Função de saída g: $S \times A \to Z$ definida por

$$\begin{array}{lll} g(s_0, a) = x, & g(s_1, a) = x, & g(s_2, a) = z \\ g(s_0, b) = y, & g(s_1, b) = z, & f(s_2, b) = y \end{array}$$

Tabela de Estados e Diagrama de Estados de uma Máquina de Estado Finito

Existem duas maneiras de representar uma máquina de estado finito de forma compacta. Uma maneira é por uma tabela conhecida como *tabela de estados* da máquina M; a outra é por um grafo orientado rotulado conhecido como *diagrama de estados* da máquina M.

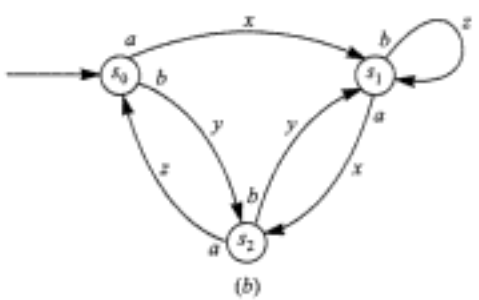
A tabela de estados combina a função de próximo estado f e a função de saída g em uma única tabela que representa a função F: $S \times A \to S \times Z$ definida por

$$F(s_i, a_j) = (f(s_i, a_j), g(s_i, a_j))$$

Por exemplo, a tabela de estados da máquina M do Exemplo 13.12 está desenhada na Figura 13-7(*a*). Os estados estão listados no lado esquerdo da tabela, com o estado inicial aparecendo em primeiro lugar, e os símbolos de entrada estão listados no topo da tabela. Cada elemento da tabela é um par (s_k, z_r) onde $s_k = f(s_i, a_j)$ é o próximo estado, e $z_r = g(s_i, a_j)$ é o símbolo de saída. Admite-se que os únicos símbolos de saída são os que aparecem na tabela.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_2, x	s_1, y
s_2	s_0, x	s_1, y

(*a*)



(*b*)

Fig. 13-7

O diagrama de estados $D = D(M)$ de uma máquina de estado finito $M = M(A, S, Z, s_0, f, g)$ é um grafo orientado rotulado. Os vértices de D são os estados de M. Ademais, se

$$F(s_i, a_j) = (s_k, z_r), \quad \text{isto é,} \quad f(s_i, a_j) = s_k \quad \text{e} \quad g(s_i, a_j) = z_r$$

então existe um arco (seta) de s_i para s_k que é rotulado com um par a_j, z_r. Normalmente, colocamos o símbolo de entrada a_j próximo à base da seta (perto de s_i) e o símbolo de saída z_r próximo ao centro da seta. Também rotulamos o estado inicial s_0 desenhando uma seta extra para s_0. Por exemplo, o diagrama de estados da máquina M do Exemplo 13.12 aparece na Figura 13-7(*b*).

Fitas de Entrada e de Saída

A discussão acima sobre uma máquina de estado finito M não mostra as propriedades dinâmicas de M. Suponha que M recebe um *string* (palavra) de símbolos de entrada, digamos,

$$u = a_1 a_2 \cdots a_m$$

Visualizamos esses símbolos em uma "fita de entrada"; a máquina M "lê" esses símbolos de entrada,

$$v = s_0 s_1 s_2 \cdots s_m$$

um por um e, simultaneamente, passa por uma seqüência de estados

$$w = z_1 z_2 \cdots z_m$$

onde s_0 é o estado inicial, enquanto imprime um *string* (palavra) de símbolos de saída em uma "fita de saída". Formalmente, o estado inicial s_0 e a cadeia de entrada u determinam as cadeias v e w por

$$s_i = f(s_{i-1}, a_i) \quad \text{e} \quad z_i = g(s_{i-1}, a_i)$$

onde $i = 1, 2, \ldots, m$.

Exemplo 13.13 Considere a máquina M da Figura 13-7, isto é, o Exemplo 13-12. Suponha que a entrada é a palavra

$$u = abaab$$

Calculamos a seqüência v de estados e a palavra de saída m a partir do diagrama de estados como segue. Começando no estado inicial s_0, seguimos as setas rotuladas pelos símbolos de entrada como a seguir:

$$s_0 \xrightarrow{a,x} s_1 \xrightarrow{b,z} s_1 \xrightarrow{a,x} s_2 \xrightarrow{a,z} s_0 \xrightarrow{b,y} s_2$$

Isso produz a seguinte seqüência de estados v e a palavra de saída w:

$$v = s_0 s_1 s_1 s_2 s_0 s_2 \quad \text{e} \quad w = xzxzy$$

Adição Binária

Esta subseção descreve uma máquina de estado finito M capaz de executar adição binária. Adicionando 0 no início dos nossos números, podemos assumir que eles têm o mesmo número de dígitos. Se à máquina for informada a entrada:

$$\begin{array}{r} 1101011 \\ +\,0111011 \\ \hline \end{array}$$

queremos, então, que a saída seja a soma binária

$$10100110$$

Especificamente, a entrada é a cadeia de pares de dígitos a ser somada:

$$11, \quad 11, \quad 00, \quad 11, \quad 01, \quad 11, \quad 10, \quad b$$

onde b denota espaço, e a saída deve ser a cadeia

$$0, \quad 1, \quad 1, \quad 0, \quad 0, \quad 1, \quad 0, \quad 1$$

Também queremos que a máquina assuma o estado chamado de "parada" quando terminar a adição.

Os símbolos de entrada são

$$A = \{00, 01, 10, 11, b\}$$

e os símbolos de saída são

$$Z = \{0, 1, b\}$$

A máquina que "construímos" terá três estados:

$$S = \{\text{vai-um}^{\dagger}\ (c),\ \text{não vai-um}\ (n),\ \text{parada}\ (s)\}$$

neste caso, n é o estado inicial. A máquina está mostrada na Figura 13-8.

Enunciamos o teorema seguinte a fim de ilustrar as limitações das nossas máquinas.

Teorema 13-5: não existe máquina de estado finito M que possa fazer operações binárias.

Se limitarmos o tamanho dos números que multiplicamos, tais máquinas existem. Computadores são importantes exemplos de máquinas finitas que multiplicam números, mas os números são limitados em seu tamanho.

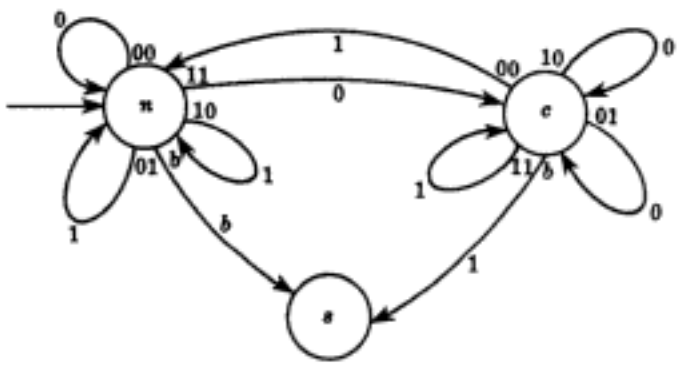


Fig. 13-8

13.8 NÚMEROS DE GÖDEL

Lembre (Seção 11.5) que um inteiro positivo $p > 1$ é dito um número primo se seus únicos divisores positivos forem 1 e p. Denote por $p_1, p_2, \ldots$ os números primos sucessivos. Logo,

$$p_1 = 2, \qquad p_2 = 3, \qquad p_3 = 5, \qquad p_4 = 7, \qquad p_5 = 11, \qquad \ldots$$

(Pelo Teorema 11.11, existe um número infinito de primos.) O teorema fundamental da aritmética (Teorema 11.19) afirma que qualquer inteiro positivo $n > 1$ pode ser escrito de maneira única (exceto pela ordem) como um produto de números primos. O lógico alemão Kurt Gödel usou esse resultado para codificar seqüências finitas de números e também para codificar palavras sobre um alfabeto finito ou enumerável. A cada seqüência ou palavra é atribuído um inteiro positivo denominado *número de Gödel* como a seguir.

† N. de T. No original, *carry*.

Hidden page

Definição 1.2: uma *expressão de fita* é uma expressão envolvendo apenas elementos do conjunto fita A.

A máquina de Turing M pode ser vista como um cabeçote de leitura/gravação de fita que se move para frente e para trás ao longo de uma fita infinita. A fita é dividida, no sentido do comprimento, em quadrados (células), e cada quadrado pode ser branco ou guardar um símbolo. A cada tempo, a máquina de Turing M está em um determinado estado interno s_i lendo um dos símbolos na fita a_j. Supomos que apenas um número finito de símbolos não brancos aparecem na fita.

A Figura 13-9(a) é uma representação gráfica de uma configuração de uma máquina de Turing M no estado s_2 lendo o segundo símbolo onde $a_1a_3Ba_1a_1$ é escrito na fita. (Note, novamente, que B é o símbolo branco.) Este desenho pode ser representado pela expressão $\alpha = a_1s_2a_3Ba_1a_1$, onde escrevemos o estado s_2 de M antes do símbolo de fita a_3 que M está lendo. Observe que α é uma expressão que usa apenas o alfabeto de fita A, exceto pelo símbolo de estado s_2 que não está no final da expressão, já que este aparece antes do símbolo de fita a_3 que M está lendo. A Figura 13-9 mostra duas outras representações gráficas de configurações e suas expressões correspondentes.

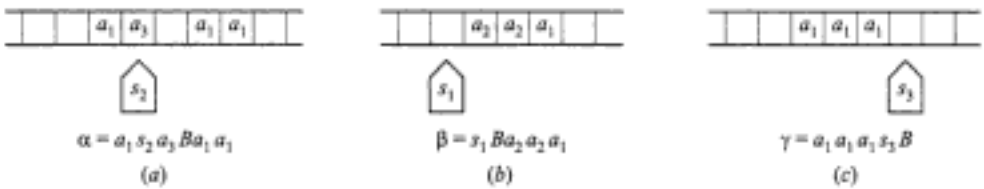


Fig. 13-9

Apresentaremos as definições formais.

Definição 1.3: uma *configuração*[†] α é uma expressão da forma

$$\alpha = Ps_ia_kQ$$

onde P e Q são expressões de fita (possivelmente vazias).

Definição 1.4: seja $\alpha = Ps_ia_kQ$ uma configuração. Dizemos que uma máquina de Turing M *está no estado* s_i *lendo*[††] *a letra* a_k, e que a *expressão na fita* é a expressão Pa_kQ, isto é, α sem o símbolo de estado s_i.

Como mencionado acima, a cada instante, a máquina de Turing M está em um certo estado s_i e lendo um símbolo de fita a_k. A máquina de Turing M é capaz de fazer as três tarefas seguintes simultaneamente:

(i) M apaga o símbolo lido a_k e escreve no seu lugar o símbolo de fita a_ℓ (onde admitimos $a_\ell = a_k$).

(ii) M muda seu estado interno s_i para o estado s_j (onde admitimos $s_j = s_i$).

(iii) M move um quadrado para a direita, move um quadrado para a esquerda ou não se move.

As ações de M mencionadas acima podem ser descritas por uma expressão com cinco letras, denominada *quíntupla*, que definimos abaixo.

Definição 1.5: uma *quíntupla* q é uma expressão de cinco letras da forma:

$$q = (s_i, a_k, a_\ell, s_j, \left\{ \begin{matrix} L \\ R \\ N \end{matrix} \right\})$$

Isto é, a primeira letra de q é um símbolo de estado, a segunda é um símbolo de fita, a terceira é um símbolo de fita, a quarta é um símbolo de estado e a última é um símbolo de direção, L, R ou N.

Apresentamos a seguir a definição formal de uma máquina de Turing.

[†] N. de T. No original, *picture*.

[††] N. de T. No original, *scanning*.

Definição 1.6: uma máquina de Turing M é um conjunto finito de quíntuplas tal que:

(i) Duas quíntuplas distintas não podem iniciar com as mesmas duas letras.

(ii) Nenhuma quíntupla começa com s_H, s_Y ou s_N.

A condição (i) da definição garante que a máquina M não pode executar mais de uma tarefa a cada tempo, e a condição (ii) garante que M pára nos estados s_H, s_Y ou s_N.

A definição seguinte é uma maneira equivalente de definir uma máquina de Turing.

Definição 1.6': uma máquina de Turing é uma função parcial de

$$S\backslash\{s_H, s_Y, s_N\} \times A \qquad \text{em} \qquad A \times S \times d$$

O termo "função parcial" significa que o domínio de M é um subconjunto de $S\backslash\{s_H, s_Y, s_N\} \times A$.

A ação da máquina de Turing descrita acima pode ser agora formalmente definida.

Definição 1.7: sejam α e β configurações. Escrevemos

$$\alpha \rightarrow \beta$$

se uma das seguintes condições ocorre, onde a, b e c são letras de fita e P e Q são expressões de fita (possivelmente vazias):

(i) $\alpha = Ps_iaQ$, $\beta = Ps_jbQ$ e M contém a quíntupla $q = s_iabs_jN$.

(ii) $\alpha = Ps_iacQ$, $\beta = Pbs_jcQ$ e M contém a quíntupla $q = s_iabs_jR$.

(iii) $\alpha = Pcs_iaQ$, $\beta = Ps_jcbQ$ e M contém a quíntupla $q = s_iabs_jL$.

(iv) $\alpha = Ps_ia$, $\beta = Pbs_jB$ e M contém a quíntupla $q = s_iabs_jR$.

(v) $\alpha = s_iaQ$, $\beta = s_jBbQ$ e M contém a quíntupla $q = s_iabs_jL$.

Observe que, em todos os cinco casos, M substitui a por b na fita (onde é permitido $b = a$), e M troca seu estado de s_i para s_j. Além disso:

(i) Neste caso, M não se move.

(ii) Neste caso, M se move para a direita.

(iii) Neste caso, M se move para a esquerda.

(iv) Neste caso, M se move para a direita; entretanto, como M está lendo a letra da extrema direita, é necessário acrescentar o símbolo de branco, B, à direita.

(v) Neste caso, M se move para a esquerda; entretanto, como M está lendo a letra da extrema esquerda, é necessário acrescentar o símbolo de branco, B, à esquerda.

Definição 1.8: uma configuração α é chamada de *terminal* se não existe configuração β tal que $\alpha \rightarrow \beta$.

Em particular, qualquer configuração α em algum dos três estados de parada deve ser terminal, já que nenhuma quíntupla começa com s_H, s_Y ou s_N.

Computação com uma Máquina de Turing

A descrição anterior é de uma máquina de Turing M estática. Discutiremos agora sua dinâmica.

Definição 1.9: uma *computação* com uma máquina de Turing M é uma seqüência de configurações $\alpha_0, \alpha_1, \ldots, \alpha_m$ tal que $\alpha_{i-1} \rightarrow \alpha_i$, para $i = 1, \ldots, m$ e α_m é uma configuração terminal.

Em outras palavras, uma computação é uma seqüência

$$\alpha_0 \rightarrow \alpha_1 \rightarrow \alpha_2 \rightarrow \cdots \rightarrow \alpha_m$$

que não pode ser estendida, uma vez que α_m é um estado terminal. Usaremos a nomenclatura $term(a)$ para denotar a configuração final de uma configuração iniciando com α. Logo, $(\alpha_0) = \alpha_m$ na computação acima.

Hidden page

Definição 2.1: cada número n será representado pela expressão de fita $\langle n\rangle$ onde $\langle n\rangle = 1^{n+1}$. Portanto,

$$\langle 4\rangle = 11111 = 1^5, \qquad \langle 0\rangle = 1, \qquad \langle 2\rangle = 111 = 1^3.$$

Definição 2.2: seja E uma expressão. Então, $[E]$ denota o número de vezes que 1 ocorre na expressão. Logo,

$$[11Bs_2a_3111Ba_4] = 5, \qquad [a_4s_2Ba_2] = 0 \qquad \text{e} \qquad [\langle n\rangle] = n + 1.$$

Definição 2.3: uma expressão $f: \mathbf{N}_0 \to \mathbf{N}_0$ é *computável* se existe uma máquina de Turing M tal que, para todo inteiro n, M pára em $\langle n\rangle$ e

$$f(n) = [\text{term}(\alpha(\langle n\rangle))]$$

Neste caso, diremos que M *computa* f.

Isto é, dados uma função f e um inteiro n, informamos como entrada $\langle n\rangle$ e usamos M. Se M sempre pára em $\langle n\rangle$ e se o número de 1s na configuração final for igual a $f(n)$, então f é uma função computável, e M computa f.

Exemplo 13.15 A função $f(n) = n + 3$ é computável. A entrada é $W = 1^{n+1}$. Logo, precisamos apenas adicionar dois 1 à entrada. Descrevemos a seguir uma máquina de Turing M que computa f.

$$M = \{q_1, q_2, q_3\} = \{s_0 1 1 s_0 L,\ s_0 B 1 s_1 L,\ s_1 B 1 s_H N\}$$

Observe que:

(1) q_1 move a máquina M para a esquerda.
(2) q_2 escreve 1 no quadrado branco B e move M para a esquerda.
(3) q_3 escreve 1 no quadrado branco B e pára M.

Conseqüentemente, para qualquer inteiro positivo n,

$$s_0 1^{n+1} \to s_0 B 1^{n+1} \to s_1 B 1^{n+2} \to s_H 1^{n+3}$$

Logo, M computa $f(n) = n + 3$. É claro que, para todo inteiro positivo k, a função $f(n) = n + k$ é computável.

Teorema 13-8: suponha que $f: \mathbf{N}_0 \to \mathbf{N}_0$ e $g: \mathbf{N}_0 \to \mathbf{N}_0$ são computáveis. A função composta $h = g \circ f$ é computável.

Indicamos aqui a prova do teorema. Suponha que M_f e M_g são as máquinas de Turing que computam f e g, respectivamente. Dada uma entrada $\langle n\rangle$, aplicamos M_f a $\langle n\rangle$ para obter ao final uma expressão E com $[E] = f(n)$. Então escrevemos que $E = s_0 1^{f(n)}$. Depois acrescentamos 1 a E para obter $E' = s_0 1 1^{f(n)}$ e aplicamos M_g a E'. Isso produzirá E'' onde $[E''] = g(f(n)) = (g \circ f)(n)$, como desejado.

Funções de Várias Variáveis

Esta subseção define uma função computável $f(n_1, n_2, \ldots, n_k)$ de k variáveis. Primeiramente precisamos representar a lista $m = (n_1, n_2, \ldots, n_k)$ no nosso alfabeto A.

Definição 2.4: cada lista $m = (n_1, n_2, \ldots, n_k)$ de k inteiros é representada pela expressão de fita $\langle m\rangle$ onde

$$\langle m\rangle = \langle n_1\rangle B\langle n_2\rangle B \cdots B\langle n_k\rangle$$

Logo, $\langle (2, 0, 4)\rangle = 111B1B11111 = 1^3B1^1B1^5$.

Definição 2.5: uma função $f(n_1, n_2, \ldots, n_k)$ de k variáveis é computável se existe uma máquina de Turing M tal que, para toda lista $m = (n_1, n_2, \ldots, n_k)$, M pára em $\langle m\rangle$ e

$$f(m) = [\text{term}(\alpha(\langle m\rangle))]$$

Neste caso, dizemos que M *computa* f.

A definição é análoga à Definição 2.3 para uma variável.

Hidden page

Hidden page

13.14 Seja $A = \{a, b\}$. Descreva a linguagem $L(r)$ onde:
(*a*) $r = abb^*a$; (*b*) $r = b^*ab^*ab^*$; (*c*) $r = ab^* \wedge a^*$.

(*a*) $L(r)$ consiste em todas as palavras começando e terminando em A e tendo no meio uma ou mais letras b.

(*b*) $L(r)$ consiste em todas as palavras com exatamente dois a.

(*c*) Neste caso, r não é exatamente uma expressão regular já que não é um dos símbolos que podem ser usados para formar expressões regulares.

13.15 Seja $A = \{a, b, c\}$ e $w = ac$. Verifique se w pertence ou não a $L(r)$ onde:
(*a*) $r = ab^*c^*$; (*b*) $r = (a^*b \vee c)^*$.

(*a*) Sim, já que $w = a\lambda c$ e $\lambda \in L(b^*)$ e $c \in L(c^*)$.

(*b*) Não. Note que $L(a^*b)$ consiste em palavras a^*b. Logo, se a aparece em uma palavra em $L(r)$, então a só pode ser seguida por a ou b, não por c.

13.16 Seja $A = \{a, b, c\}$ e seja $w = abc$. Verifique se w pertence ou não a $L(r)$ onde:
(*a*) $r = a^* \vee (b \vee c)^*$; (*b*) $r = a^*(b \vee c)^*$.

(*a*) Não. Neste caso, $L(r)$ consiste nas palavras em a ou palavras em b e c.

(*b*) Sim, pois $a \in L(a^*)$ e $bc \in (b \vee c)^*$.

13.17 Seja $A = \{a, b\}$. Ache uma expressão regular r tal que $L(r)$ consista em todas as palavras w onde:
(*a*) w começa com a^2 e termina com b^2. (*b*) w contém um número par de letras as.

(*a*) Seja $r = a^2(a \vee b)^*b^2$.

(*b*) Note que $s = b^*ab^*ab^*$ consiste em todas as palavras com exatamente dois as. Logo, $r = s^* = (b^*ab^*ab^*)^*$.

Autômatos Finitos, Máquinas de Estado Finito

13.18 Seja M um autômato com conjunto de entrada A, conjunto de estados S e conjunto de estados de aceite ("sim") Y descritos a seguir:

$$A = \{a, b\}, \qquad S = \{s_0, s_1, s_2\}, \qquad Y = \{s_1\}$$

Suponha que s_0 é o estado inicial de M, e que a função de próximo estado, F, de M é dada pela tabela da Figura 13-10(*a*).

(*a*) Desenhe o diagrama de estados $D = D(M)$ de M.

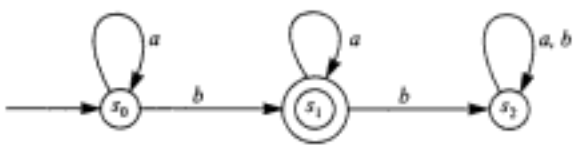
(*b*) Descreva a linguagem $L = L(M)$ aceita por M.

(*a*) O diagrama de estados D aparece na Figura 13-10(*b*). Os vértices de D são os estados com um círculo duplo indicando um estado de aceitação. Se $F(s_j, x) = s_k$, existe uma aresta orientada de s_j para s_k rotulada pelo símbolo de entrada x. Além disso, existe uma aresta especial que termina no estado inicial s_0.

(*b*) $L(M)$ consiste em todas as palavras w com exatamente um b. Especificamente, se uma palavra de entrada não tiver b, então ela termina em s_0, e se w tiver dois ou mais bs ela termina em s_2. Em qualquer outra condição, w termina em s_1, que é o único estado de aceite.

F	a	b
s_0	s_0	s_1
s_1	s_1	s_2
s_2	s_2	s_2

(*a*)



(*b*)

Fig. 13-10

13.19 Seja $A = \{a, b\}$. Construa um autômato M que aceitará precisamente as palavras de A que têm um número par de as. Por exemplo, *aababbab*, *aa*, *bbb*, *ababaa* serão aceitas por M, mas *ababa*, *aaa*, *bbabb* serão rejeitadas.

Precisamos apenas de dois estados, s_0 e s_1. Assumimos que M está no estado s_0 ou s_1 dependendo do número de letras a, até o passo em questão, ser par ou ímpar. Além disso, s_0 é o estado inicial. O diagrama de estados de M aparece na Figura 13-11.

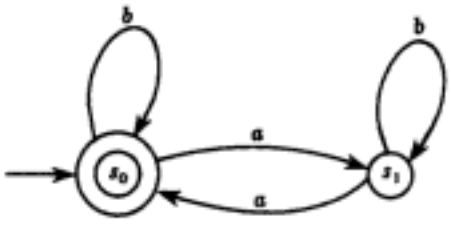


Fig. 13-11

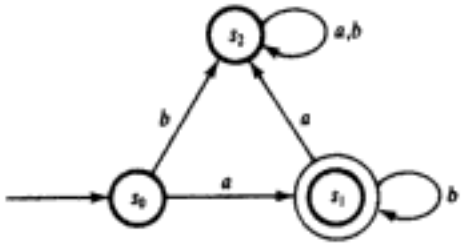


Fig. 13-12

13.20 Seja $A = \{a, b\}$. Construa um autômato M que aceitará as palavras de A que comecem com a seguido de um ou mais bs.

Veja a Figura 13-12.

13.21 Descreva as palavras w na linguagem L aceitas pelo autômato M da Figura 13-13.

O sistema só pode atingir um estado de aceite s_2 quando existe um a em w que segue um b.

13.22 Descreva as palavras w na linguagem L aceitas pelo autômato M da Figura 13-14.

A presença de um a em w não muda o estado do sistema, mas cada b em w muda o estado de s_i para s_{i+1} (mod 4). Portanto, w é aceita por M se o número n de bs em w é congruente a 3 módulo 4, isto é, $n = 3, 7, 11, \ldots$

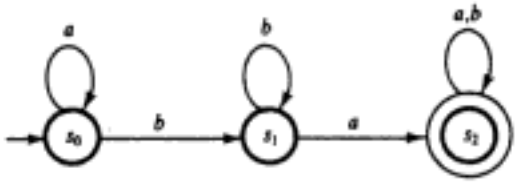


Fig. 13-13

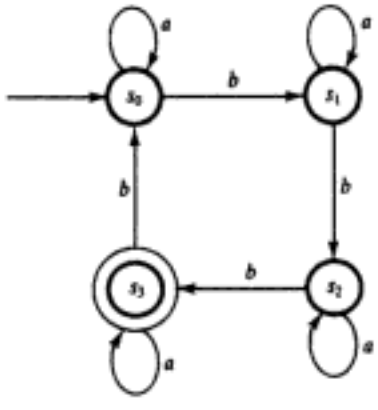


Fig. 13-14

13.23 Suponha que L é uma linguagem sobre A que é aceita pelo autômato $M = \langle A, S, Y, s_0, F\rangle$. Ache um autômato N que aceita L^c, isto é, as palavras de A que não pertencem a L.

Simplesmente troque os estados de aceitação e rejeição em M para obter N. Então, w será aceita na nova máquina N se e somente se for rejeitada por M, isto é, se e somente se w pertence a L^c. Formalmente, $N = \langle A, S, S \backslash Y, s_0, F\rangle$.

13.24 Sejam $M = \langle A, S, Y, s_0, F\rangle$ e $M' = \langle A, S', Y', s_0', F'\rangle$ autômatos sobre o mesmo alfabeto A que aceitam as linguagens $L(M)$ e $L(M')$, respectivamente. Construa um autômato N sobre A que aceita precisamente $L(M)\cap L(M')$.

Considere $S \times S'$ como o conjunto de estados de N. Defina (s, s') como um estado de aceite de N se s e s' são estados de aceite em M e M', respectivamente; escolha (s_0, s_0') como estado inicial de N. Tome a função de próximo-estado de N, G: $(S \times S') \times A \to (S \times S')$ definida como

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Então, N aceitará exatamente as palavras de $L(M)\cap L(M')$.

13.25 Repita o Problema 13.24 fazendo, agora, N aceitar as palavras de $L(M)\cup L(M')$.

Novamente, considere $S \times S'$ como conjunto de estados de N, e seja (s_0, s_0') o estado inicial de N. Agora considere $(S \times Y') \cup (Y \times S')$ os estados de aceite em N. A função de próximo-estado será mais uma vez definida como

$$G((s, s'), a) = (F(s, a), F'(s', a))$$

Então, N aceitará precisamente as palavras em $L(M)\cup L(M')$.

13.26 Seja M a máquina de estado finito cuja tabela de estados aparece na Figura 13-15(a).

(a) Ache o conjunto de entrada A, o conjunto de estados S, o conjunto de saída Z e o estado inicial.

(b) Desenhe o diagrama de estados $D = D(M)$ de M.

(c) Suponha que $w = aababaabbbab$ é uma palavra de entrada (*string*). Ache a palavra de saída correspondente v.

(a) Os símbolos de entrada estão no topo da tabela. Os estados estão listados à esquerda, e os símbolos de saída aparecem na tabela. Logo,

$$A = \{a, b\} \qquad S = \{s_0, s_1, s_2, s_3\}, \qquad Z = \{x, y, z\}$$

O estado s_0 é o estado inicial uma vez que é o primeiro estado listado na tabela.

(b) O diagrama de estados $D = D(M)$ aparece na Figura 13-15(b). Note que os vértices de D são os estados de M.

Suponha que

$$F(s_i, a_j) = (s_k, z_r), \qquad \text{isto é,} \qquad f(s_i, a_j) = s_k \qquad \text{ou} \qquad g(s_i, a_j) = z_r$$

Então, existe uma aresta orientada de s_i para s_k rotulada pelo par a_j, z_r. Normalmente, o símbolo de entrada a_j é colocado próximo à base da seta (perto de s_i), e o símbolo de saída z_r é colocado perto do centro da seta.

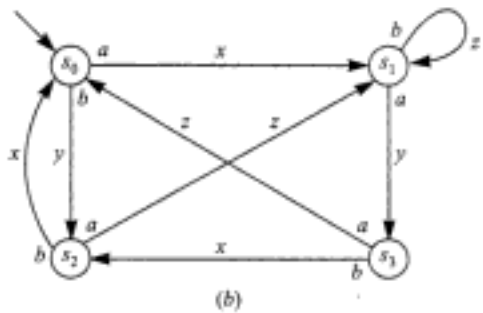
(c) Saindo do estado inicial s_0, movemo-nos de estado para estado através das setas que são, respectivamente, rotuladas pelos símbolos de entrada dados a seguir:

$$s_0 \xrightarrow{a} s_1 \xrightarrow{a} s_3 \xrightarrow{b} s_2 \xrightarrow{a} s_1 \xrightarrow{b} s_1 \xrightarrow{a} s_3 \xrightarrow{a} s_0 \xrightarrow{b} s_2 \xrightarrow{b} s_0 \xrightarrow{a} s_1 \xrightarrow{b} s_1$$

Os símbolos de saída nas setas acima produzem a palavra de saída desejada $v = xyzzyzyxxz$.

F	a	b
s_0	s_1, x	s_2, y
s_1	s_3, y	s_1, z
s_2	s_1, z	s_0, x
s_3	s_0, z	s_2, x

(a)



(b)

Fig. 13-15

Gramáticas

13.27 Defina: (*a*) gramática livre de contexto; (*b*) gramática regular.

(*a*) Uma gramática livre de contexto é o mesmo que uma gramática do Tipo 2, isto é, toda produção é da forma $A \to \beta$, isto é, o lado esquerdo é uma única variável, e o lado direito é uma palavra com um ou mais símbolos.

(*b*) Uma gramática regular é o mesmo que uma gramática do Tipo 3, isto é, toda produção é da forma $A \to a$ ou $A \to aB$, isto é, o lado esquerdo é uma única variável, e o lado direito é um terminal ou um terminal seguido de uma variável.

13.28 Ache a linguagem $L(G)$ gerada pela gramática G com variáveis S, A, B, terminais a, b e produções $S \to aB$, $B \to b$, $B \to bA$, $A \to aB$.

Observe que podemos usar a primeira produção apenas uma vez, já que o símbolo de *start* S não aparece em outro lugar. Ademais, só podemos obter uma palavra terminal usando a segunda produção. Em outras situações podemos, como alternativa, adicionar letras a e b usando a terceira e a quarta produção. Em outras palavras,

$$L(G) = \{(ab)^n = abab\cdots ab : n \in \mathbf{N}\}$$

13.29 Seja L o conjunto de todas as palavras em a e b com um número par de as. Ache a gramática G que irá gerar L.

Afirmamos que a gramática G com as seguintes produções gerará L:

$$S \to aA, \quad S \to bB, \quad B \to bB, \quad B \to aA, \quad A \to aB, \quad A \to bA, \quad A \to a, \quad B \to b$$

Observe que a soma dos as e As, em qualquer palavra α, ou não se altera ou aumenta em 2 quando qualquer produção é aplicada a α. Logo, qualquer palavra w nos terminais a e b que seja derivada de S conterá um número par de as. Em outras palavras, $L(G) \subseteq L$. Por outro lado, fica claro quais produções deveriam ser usadas para escrever qualquer palavra v em L; isto é, usamos $S \to aA$ ou $S \to bB$, dependendo de b começar com a ou b, e usamos $A \to aB$ ou $B \to aA$ se qualquer letra subseqüente for um a, e usamos $A \to bA$ ou $B \to bB$ se qualquer letra subseqüente for um b. Como última letra de v, usamos $A \to a$ ou $B \to b$. Logo, $L(G) = L$.

13.30 Determine o tipo de gramática G que consiste nas produções:

(*a*) $S \to aA$, $A \to aAB$, $B \to b$, $A \to a$.

(*b*) $S \to aAB$, $AB \to bB$, $B \to b$, $A \to aB$.

(*c*) $S \to aAB$, $AB \to a$, $A \to b$, $B \to AB$.

(*d*) $S \to aB$, $B \to bA$, $B \to b$, $B \to a$, $A \to aB$, $A \to a$.

(*a*) Cada produção é da forma $A \to \alpha$, isto é, uma variável à esquerda; logo, G é uma gramática livre de contexto ou do Tipo 2.

(*b*) O comprimento do lado esquerdo de cada produção não excede o comprimento do lado direito; logo, G é uma gramática do Tipo 1.

(*c*) A produção $AB \to a$ significa que G é uma gramática do Tipo 0.

(*d*) G é uma gramática regular do Tipo 3, pois cada produção é da forma $A \to a$ ou $A \to aB$.

13.31 Seja L a linguagem em A que consiste em todas as palavras w com exatamente um b, isto é,

$$L = \{b, a^r b, \ ba^s, \ a^r ba^s : r > 0, \ s > 0\}.$$

(*a*) Ache uma expressão regular r tal que $L = L(r)$.

(*b*) Ache uma gramática regular G que gera a linguagem L.

(*a*) Seja $r = a^*ba^*$. Então, $L(r) = L$.

(*b*) A gramática regular G com as produções seguintes gera L:

$$S \to (b, aA), \qquad A \to (b, aA, bB), \qquad B \to (a, aB)$$

Isto é, a letra b só pode aparecer uma vez em cada palavra derivada de S. G é regular, já que tem a forma desejada.

13.32 Seja L a linguagem em $A = \{a, b, c\}$ que consiste em todas as palavras da forma $w = a^r b^s c^t$ onde $r, s, t > 0$, isto é, *as* seguidos por *bs* seguidos por *cs*.

(*a*) Ache uma expressão regular r tal que $L = L(r)$.

(*b*) Ache uma gramática regular G que gera a linguagem L.

(*a*) Seja $r = aa^*bb^*cc^*$. Então, $L = L(r)$.

(*b*) A gramática regular G com as seguintes produções gera L:

$$S \to aA, \qquad A \to (aA, bB), \qquad B \to (bB, c, cC), \qquad C \to (c, cC)$$

13.33 Considere a gramática regular G com as produções

$$S \to aA, \qquad A \to aB, \qquad B \to bB, \qquad B \to a$$

(*a*) Ache a árvore de derivação da palavra $w = aaba$.

(*b*) Descreva todas as palavras w na linguagem L gerada por G.

(*a*) Note primeiro que w pode ser derivada de S como a seguir:

$$S \Rightarrow aA \Rightarrow a(aB) \Rightarrow aa(bB) \Rightarrow aaba$$

A Figura 13-16 mostra a árvore de derivação correspondente.

(*b*) Usando as produções 1, depois 2 e depois 3, r vezes, e 4, derivamos a palavra $w = aab^r a$ onde $r \geq 0$. Nenhuma outra palavra pode ser derivada de S.

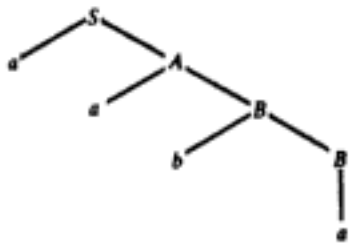


Fig. 13-16

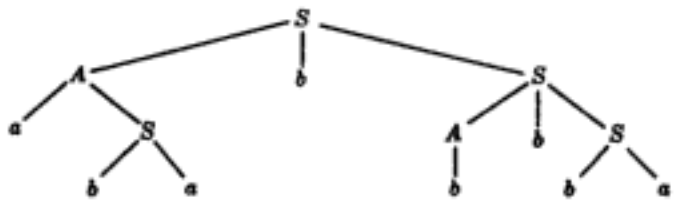


Fig. 13-17

13.34 A Figura 13-17 é a árvore de derivação de uma palavra w em uma linguagem L de uma gramática livre de contexto G. (*a*) Ache w. (*b*) Quais terminais, variáveis e produções devem estar em G?

(*a*) A seqüência de folhas da esquerda para a direita produz a palavra $w = ababbbba$.

(*b*) As folhas mostram que a e b devem ser terminais, e os vértices internos mostram que S e A devem ser variáveis, sendo S a variável de *start*. Os filhos de cada variável mostram que $S \to AbS$, $A \to aS$, $S \to ba$ e $A \to b$ devem ser produções.

13.35 Existe uma árvore de derivação para qualquer palavra w derivada do símbolo de *start* S em uma gramática G?

Não. Árvores de derivação só existem para gramáticas dos Tipos 2 e 3, isto é, para gramáticas livres de contexto e gramáticas regulares.

13.36 Reescreva cada gramática G do Problema 13.30 na forma de Backus-Naur.

A forma de Backus-Naur só se aplica a gramáticas livres de contexto (o que inclui gramáticas regulares). Portanto, apenas (*a*) e (*d*) podem ser escritas na forma de Backus-Naur. A forma é obtida como a seguir:

(i) Troque $\to$ por $::=$.

(ii) Delimite não-terminais com $\langle\ \rangle$.

(iii) Todas as produções com o mesmo lado esquerdo são combinadas em uma única declaração com todos o lados direitos listados à direita de $::=$ separados por barras verticais.

Conseqüentemente,

(*a*) $\langle S\rangle ::= a\langle A\rangle,\ \langle A\rangle ::= a\langle A\rangle\langle B\rangle | a,\ \langle B\rangle ::= b.$

(*d*) $\langle S\rangle ::= a\langle B\rangle,\ \langle B\rangle ::= b\langle A\rangle | b | a,\ \langle A\rangle ::= a\langle B\rangle | a.$

Máquinas de Turing

13.37 Seja M uma máquina de Turing. Determine a configuração α correspondente a cada situação.

(*a*) M está no estado s_3 e lendo a terceira letra da expressão de fita $w = aabca$.

(*b*) M está no estado s_2 e lendo a última letra da expressão de fita $w = abca$.

(*c*) A entrada é a expressão de fita $w = 1^4B1^2$.

A configuração é obtida colocando o símbolo de estado antes da letra da fita que está sendo lida. Inicialmente, M está no estado s_0 lendo a primeira letra de uma entrada. Logo:

(*a*) $\alpha = aas_3bca$ (*b*) $\alpha = abcs_2a$; (*c*) $\alpha = s_0 1111B11$.

13.38 Suponha que $\alpha = aas_2ba$ é uma configuração. Ache β tal que $\alpha \rightarrow \beta$ se a máquina de Turing M tem a quíntupla q onde:

(*a*) $q = s_2bas_1L$; (*b*) $q = s_2bbs_3R$; (*c*) $q = s_2bas_2N$; (*d*) $q = s_3abs_1L$.

(*a*) Neste caso, M apaga b e escreve a, muda seu estado para s_1 e se move para a esquerda. Logo, $\beta = as_1aaa$.

(*b*) Neste caso, M não muda a letra lida b, muda seu estado para s_3 e se move para a direita. Logo, $\beta = aabs_3a$.

(*c*) Neste caso, M apaga b e escreve a, mantém seu estado s_2 e não se move. Logo, $\beta = aas_2aa$.

(*d*) Neste caso, q não tem efeito sobre α, pois q não começa com s_2b.

13.39 Seja $A = \{a, b\}$ e seja $L = \{a^r b^s : r > 0, s > 0\}$, isto é, L consiste em todas as palavras W começando com uma ou mais letras as e seguidas por um ou mais bs. Ache uma máquina de Turing M que reconhece L.

A estratégia é a de que queremos que M (1) mova-se para a direita sobre a, (2) mova-se para a direita sobre b (3) pare no estado aceite s_Y quando encontrar o símbolo branco B. As seguintes quíntuplas fazem isto:

$$q_1 = s_0aas_1R, \qquad q_2 = s_1aas_1R, \qquad q_3 = s_1bbs_2R, \qquad q_4 = s_2bbs_2R, \qquad q_5 = s_2BBs_YR$$

Especificamente, q_1 e q_2 fazem (1), q_3 e q_4 fazem (2) e q_5 faz (3).

Entretanto, também queremos que M não aceite uma palavra de entrada W que não pertence a L. Logo, também precisamos das quíntuplas

$$q_6 = s_0BBs_NR, \qquad q_7 = s_0bbs_NR, \qquad q_8 = s_1BBs_NR, \qquad q_9 = s_2aas_NR$$

Note que q_6 é usada se a entrada $W = \lambda = B$, a palavra vazia; q_7 é usada se a entrada W é uma expressão começando por b; q_8 é usada se a entrada W contém apenas as e q_9 é usada se a entrada W contém uma letra a seguindo uma letra b.

13.40 Ache uma máquina de Turing M que reconhece a linguagem $L = (ab)^* = \{(ab)^n : n \geq 0\}$.

Dada uma entrada W, a estratégia é fazer com que M apague o primeiro a, o último b, o primeiro a, o último b, e assim por diante. Se todas as letras são apagadas, então M aceita W, já que W pertence a L. Caso contrário, queremos que M não aceite (rejeite) W. Conseqüentemente, M precisa das seguintes 17 quíntuplas:

(1) No estado inicial s_0, M apaga o primeiro a e vai para o estado s_1, ou M aceita W se $W = \lambda$, ou rejeita W se W começar com b:

$$q_1 = s_0aBs_1R, \qquad q_2 = s_0BBs_YR, \qquad q_3 = s_0bbs_NR$$

(2) No estado s_1, M se move para a direita por todos os as até encontrar um b e entrar no estado s_2, ou M rejeita W se não existir b:

$$q_4 = s_1aas_1R, \qquad q_5 = s_1bbs_2R, \qquad q_6 = s_1BBs_NR$$

(3) No estado s_2, M se move para a direita por todos os bs até encontrar um B e entrar no estado s_3 e se mover para a esquerda, ou M rejeita W se M encontrar a:

$$q_7 = s_2bbs_2R, \qquad q_8 = s_2BBs_3L, \qquad q_9 = s_2aas_NR$$

(4) M no estado s_3 apaga o último b e depois entra no estado s_4 e se move para a esquerda:

$$q_{10} = s_3bBs_4L$$

(5) M no estado s_4 pára no estado s_Y (sucesso) se M encontra B ou M se move para a esquerda passando o b da extrema direita no estado s_5:

$$q_{11} = s_4BBs_YL, \qquad q_{12} = s_4bbs_5L$$

(6) M no estado s_5 se move para a esquerda através dos b até que M encontra um a ou rejeita W se existir um B:

$$q_{13} = s_5bbs_5L, \qquad q_{14} = s_5aas_6L, \qquad q_{15} = s_5BBs_NL$$

(7) No estado s_6, M se move para a esquerda através dos a e volta ao estado inicial s_0 quando encontra B:

$$q_{16} = s_6aas_6L, \qquad q_{17} = s_6BBs_0R$$

Funções Computáveis

13.41 Ache $\langle m\rangle$ se: (i) $m = 5$; (ii) $m = (4, 0, 3)$; (iii) $m = (3, -2, 5)$.

Lembre que $\langle n\rangle = 1^{n+1} = 11^n$ e $\langle\langle n_1, n_2, \ldots, n_r\rangle\rangle = \langle n_1\rangle B\langle n_2\rangle B \cdots B\langle n_r\rangle$. Portanto,

(*a*) $\langle m\rangle = 1^6 = 111111$.

(*b*) $\langle m\rangle = 1^5B1^1B1^4 = 11111B1B1111$.

(*c*) $\langle m\rangle$ não é definido para inteiros não negativos.

13.42 Ache $[E]$ para as expressões:

(*a*) $E = a11s_2Bb111$.

(*b*) $E = aas_3bb$.

(*c*) $E = \langle m\rangle$ onde $m = (4, 1, 2)$.

(*d*) $E = \langle m\rangle$ onde $m = (n_1, n_2, \ldots, n_r)$.

Lembre que $[E]$ conta o número de 1 em E. Logo:

(*a*) $[E] = 5$

(*b*) $[E] = 0$

(*c*) $[E] = 10$ já que $E = 1^5B1^2B1^3$

(*d*) $[E] = n_1 + n_2 + \cdots + n_r + r$ uma vez que o número de 1 com que cada n_k contribui para E é $n_k + 1$.

13.43 Seja f a função $f(n) = n - 1$ se $n > 0$ e $f(0) = 0$. Mostre que f é computável.

Precisamos determinar uma máquina de Turing M que computa f. Especificamente, queremos que M apague dois 1s na entrada de $\langle n\rangle$ quando $n > 0$, mas apenas um 1 quando $n > 0$. Isso é executado pelas quíntuplas:

$$q_1 = s_01Bs_1R, \qquad q_2 = s_1BBs_HN, \qquad q_3 = s_11Bs_HN$$

Aqui, q_1 apaga o primeiro 1 e move M para a direita. Se existir apenas um 1, então M lê um símbolo branco B e q_2 diz ao computador para parar. Caso contrário, q_3 apaga o segundo 1 e pára M.

13.44 Seja $f(x, y) = y$. Mostre que f é computável.

Precisamos achar uma máquina de Turing M que compute f. Especificamente, queremos que M apague todos os 1s de $\langle x\rangle$ e um dos 1s de $\langle y\rangle$. Isto é feito pelas quíntuplas:

$$q_1 = s_01Bs_0R, \qquad q_2 = s_0BBs_1R, \qquad q_3 = s_11Bs_HN$$

Aqui, q_1 apaga todos os 1s de $\langle x\rangle$ e um dos 1s de $\langle y\rangle$ enquanto move M para a direita. Quando M lê B, q_2 muda o estado de M de s_0 para s_1 e move M para a direita. Então, q_3 apaga o primeiro 1 em $\langle y\rangle$ e pára M.

Problemas Complementares

Palavras

13.45 Considere as palavras $u = ab^2a^3$ e $v = aba^2b^2$. Ache: (*a*) uv; (*b*) vu; (*c*) u^2; (*d*) λu; (*e*) $v\lambda v$.

13.46 Para as palavras $u = ab^2a^3$ e $v = aba^2b^2$, ache: $|u|$, $|v|$, $|uv|$, $|vu|$ e $|v^2|$.

13.47 Seja $w = abcde$. (*a*) Ache todas as subpalavras de w. (*b*) Quais delas são segmentos iniciais?

13.48 Suponha que $u = a_1a_2 \cdots a_r$, com a_k distintos. Ache o número n de subpalavras de u.

Linguagens

13.49 Sejam $L = \{a^2, ab\}$ e $K = \{a, ab, b^2\}$. Ache: (*a*) LK; (*b*) KL; (*c*) $L \vee K$; (*d*) $K \vee L$.

13.50 Seja $L = \{a^2, ab\}$. Ache: (*a*) L^0; (*b*) L^2; (*c*) L^3.

13.51 Seja $A = [a, b, c]$. Descreva L^* se: (*a*) $L = \{a^2\}$; (*b*) $L = \{a, b^2\}$; (*c*) $L = \{a, b^2, c^3\}$.

13.52 Será que $(L^2)^* = (L^*)^2$? Se não, como eles se relacionam?

13.53 Considere um alfabeto enumerável $A = \{a_1, a_2, \ldots\}$. Seja L_k a linguagem sobre A consistindo nas palavras w tais que a soma dos índices das letras em w é igual a k. (Veja o Problema 13.12). Ache: (*a*) L_3; (*b*) L_5.

Expressões Regulares, Linguagens Regulares

13.54 Seja $A = [a, b, c]$. Descreva a linguagem $L(r)$ para cada expressão regular:
(*a*) $r = ab^*c$; (*b*) $r = (ab \vee c)^*$; (*c*) $r = ab \vee c^*$

13.55 Seja $A = [a, b]$. Ache uma expressão regular r tal que $L(r)$ consiste em todas as palavras w tais que:

(*a*) w contém exatamente três letras a.

(*b*) O número de letras a é divisível por 3.

(*c*) w começa e termina em b e bab nunca é subpalavra de w; isto é, a cada ocorrência de a em w, seu expoente é maior ou igual a 2.

13.56 Seja $A = [a, b, c]$ e seja $w = ac$. Decida se w pertence ou não a $L(r)$ onde:
(*a*) $r = a^*bc^*$; (*b*) $r = a^*b^*c$; (*c*) $r = (ab \vee c)^*$.

13.57 Seja $A = [a, b, c]$ e seja $w = ac$. Decida se w pertence ou não a $L(r)$ onde:
(*a*) $r = ab^*(bc)^*$; (*b*) $r = a^* \vee (b \vee c)^*$; (*c*) $a^*b(bc \vee c^2)^*$.

Autômatos Finitos

13.58 Seja $A = [a, b]$. Construa um autômato M tal que $L(M)$ consistirá nas palavras w tais que o número de letras b seja divisível por 3. (Sugestão: são necessários três estados.)

13.59 Seja $A = [a, b]$. Construa um autômato M tal que $L(M)$ consistirá nas palavras w que começam com a e terminam com b.

13.60 Seja $A = [a, b]$. Construa um autômato M que aceite a linguagem $L(M) = \{a^rb^s : r > 0, s > 0\}$.

13.61 Seja $A = [a, b]$. Construa um autômato M que aceite a linguagem $L(M) = \{b^rab^s : r > 0, s > 0\}$.

13.62 Seja $A = [a, b]$. Construa um autômato M tal que $L(M)$ consistirá em todas as palavras nas quais o número de as seja divisível por 2, e o número de letras b seja divisível por 3. (Sugestão: use os Problemas 13.19, 13.58 e 13.24.)

Hidden page

Gramáticas

13.67 Determine o tipo de gramática G que consiste nas produções:

(*a*) $S \to aAB;\ S \to AB;\ A \to a;\ B \to b.$

(*b*) $S \to aB;\ B \to AB;\ aA \to b;\ A \to a;\ B \to b.$

(*c*) $S \to aB;\ B \to bB;\ B \to bA;\ A \to a;\ B \to b.$

13.68 Ache a gramática regular G que gera a linguagem L que consiste em todas as palavras em a e b tais que dois *as* não apareçam em posições contíguas.

13.69 Ache uma gramática livre de contexto G que consiste em todas as palavras em a e b contendo tantos *as* quanto o dobro do número de *bs*.

13.70 Ache uma gramática G que gera a linguagem L que consiste em todas as palavras da forma $a^n b a^n$ com $n \geq 0$.

13.71 Mostre que a linguagem G do Problema 13-70 não é regular.

13.72 Descreva a linguagem $L = L(G)$ onde G tem as produções $S \to aA$, $A \to bbA$, $A \to c$.

13.73 Descreva a linguagem $L = L(G)$ onde G tem as produções $S \to aSb$, $Sb \to bA$, $abA \to c$.

13.74 Escreva cada gramática G do Problema 13-67 na forma de Backus-Naur.

13.75 Seja G a gramática livre de contexto com produções $S \to (a, aAS)$ e $A \to bS$. (*a*) Escreva G na forma de Backus-Naur. (*b*) Ache a árvore de derivação da palavras $w = abaabaa$.

13.76 A Figura 13-22 é a árvore de derivação de uma palavra w em uma linguagem L de uma gramática livre de contexto G. (*a*) Ache w. (*b*) Quais terminais, variáveis e produções devem pertencer a G?

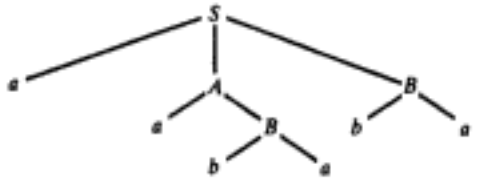


Fig. 13-22

Máquinas de Turing

13.77 Seja M uma máquina de Turing. Determine a configuração α correspondendo a cada uma das situações:

(*a*) M está no estado s_2 e lendo a terceira letra da expressão de fita $w = abbaa$.

(*b*) M está no estado s_3 e lendo a última letra da expressão de fita $w = aabb$.

(*c*) A entrada é a palavra $W = a^3b^3$.

(*d*) A entrada é a expressão de fita $W = \langle(3,2)\rangle$.

13.78 Suponha que $\alpha = abs_2aa$ é uma configuração. Ache β tal que $\alpha \to \beta$ se a máquina de Turing M tem a quíntupla q onde:

(*a*) $q = s_2abs_1R$. (*b*) $q = s_2aas_3L$. (*c*) $q = s_2abs_2N$.

(*d*) $q = s_2abs_3L$. (*e*) $q = s_3abs_2R$. (*f*) $q = s_2aas_2N$.

13.79 Repita o Problema 13.78 para a configuração $\alpha = s_2aBab$.

13.80 Ache configurações distintas α e β e uma máquina de Turing M tal que a seqüência

$$\alpha \to \beta \to \alpha \to \beta \to \cdots$$

não termine.

13.81 Suponha que $\alpha \to \beta_1$ e $\alpha \to \beta_2$. É necessário que $\beta_1 = \beta_2$?

Hidden page

13.57 (*a*) Sim; (*b*) não; (*c*) não.

13.58 Veja a Figura 13-23.

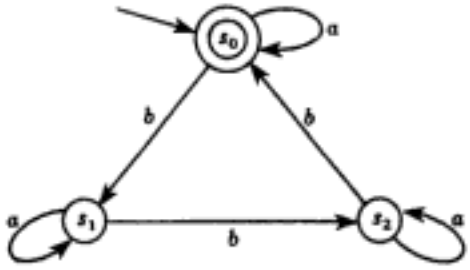


Fig. 13-23

13.59 Veja a Figura 13-24.

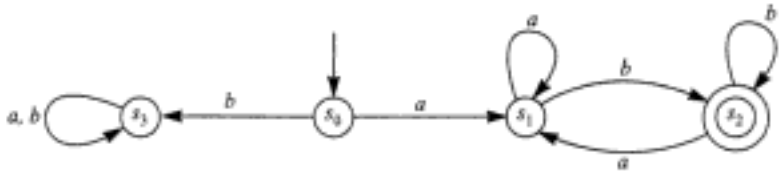


Fig. 13-24

13.60 Veja a Figura 13-25.

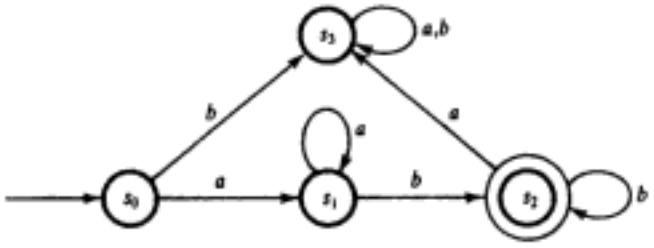


Fig. 13-25

13.61 Veja a Figura 13-26.

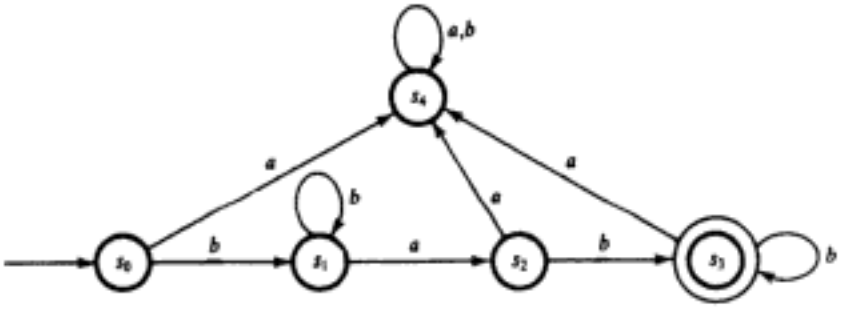


Fig. 13-26

13.62 Veja a Figura 13-27.

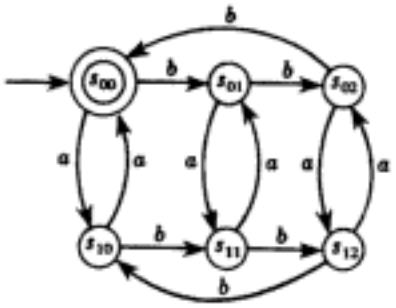


Fig. 13-27

13.63 $L(M)$ consiste em todas as palavras w que contêm $aabb$ como subpalavra.

13.64 (*a*) $A = \{a, b\}$, $S = \{s_0, s_1, s_2, s_3\}$, $Z = \{x, y, z\}$ e s_0 é o estado inicial.

(*b*) Veja a Figura 13-28.

(*c*) $v = y^2zyxzxyz$.

13.65 (*a*) Veja a Figura 13.29. (*b*) $v = xy^2xz^3xyx$.

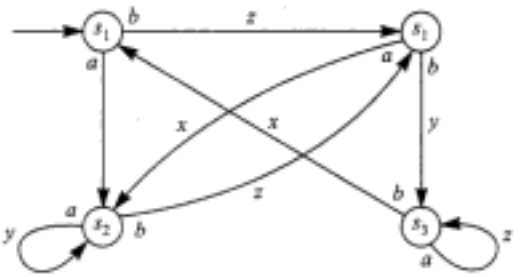


Fig. 13-28

F	a	b	c
s_0	s_1, x	s_2, z	s_1, x
s_1	s_1, y	s_2, z	s_0, z
s_0	s_1, z	s_2, x	s_0, x

Fig. 13-29

13.66 (*a*) $v = xyzxy^2z^2x^2z^2y^2$; (*b*) $v = zyxy^2zx^2zxy^2xy$.

13.67 (*a*) Tipo 2; (*b*) Tipo 0; (*c*) Tipo 3.

13.68 $S \to (a, b, aB, bA)$, $A \to (bA, ab, a, b)$, $B \to (b, bA)$.

13.69 $S \to (AAB,\ ABA,\ BAA)$, $A \to (a, BAAA,\ ABAA,\ AABA,\ AAAB)$,
$B \to (b,\ BBAA,\ BABA, aBAAB,\ ABAB,\ AABB)$.

13.70 $S \to (aSa, b)$.

13.72 $L = \{ab^{2n}c : n \geq 0\}$.

13.73 $L = \{a^ncb^n : n > 0\}$.

13.74 (*a*) $\langle S\rangle ::= a\langle A\rangle\langle B\rangle|\langle A\rangle\langle B\rangle$, $\langle A\rangle ::= a$, $\langle B\rangle ::= b$.

(*b*) Não é definida para linguagens do Tipo 0.

(*c*) $\langle S\rangle ::= a\langle B\rangle$, $\langle B\rangle ::= b\langle B\rangle|b\langle A\rangle$, $\langle A\rangle ::= a|b$.

13.75 (*a*) $\langle S\rangle ::= a|a\langle A\rangle\langle S\rangle$, $\langle A\rangle ::= b\langle S\rangle$; (*b*) Veja a Figura 13-30.

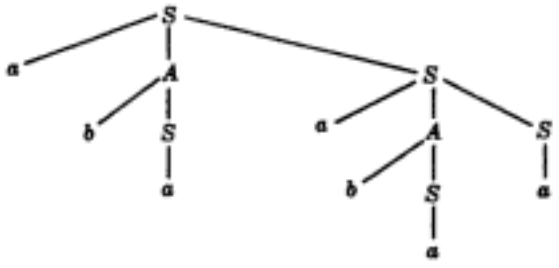


Fig. 13-30

13.76 (*a*) $w = aababa$; (*b*) $S \rightarrow aAB$, $A \rightarrow aB$, $B \rightarrow ba$.

13.77 (*a*) $\alpha = abs_2baa$; (*b*) $\alpha = aabs_3b$; (*c*) $\alpha = s_0aaabbb$; (*d*) $\alpha = s_0 1111B111$.

13.78 (*a*) $\beta = abbs_1a$; (*b*) $\beta = as_3baa$; (*c*) $\beta = abs_2ba$; (*d*) $\beta = as_3bba$; (*e*) α não é alterada por q; (*f*) $\beta = \alpha = abs_2aa$.

13.79 (*a*) $\beta = bs_1Bab$; (*b*) $\beta = s_2BaBab$; (*c*) $\beta = s_2bBab$; (*d*) $\beta = s_3BbBab$; (*e*) α não é alterada por q; (*f*) $\beta = \alpha = s_2aBab$.

13.80 $\alpha = s_0a$; $\beta = s_1b$, $q_1 = s_0abs_1N$; $q_2 = s_1Bas_0N$.

13.81 Sim.

13.82 Não, pois $\alpha \rightarrow \beta \rightarrow \alpha \rightarrow \beta \rightarrow \ldots$ nunca termina.

13.83 $q_1 = s_0BBs_NR$ (NÃO); $q_2 = s_0bbs_NR$ (NÃO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_NR$ (NÃO);
$q_5 = s_1aas_NR$ (NÃO); $q_6 = s_1bbs_2R$; $q_7 = s_2bbs_2R$;
$q_8 = s_2aas_NR$ (NÃO); $q_9 = s_2BBs_YR$ (SIM).

13.84 $q_1 = s_0BBs_NR$ (NÃO); $q_2 = s_0bbs_NR$ (NÃO);
$q_3 = s_0aas_1R$; $q_4 = s_1BBs_YR$ (aceita);
$q_5 = s_1bbs_NR$ (NÃO); $q_6 = s_1aas_2R$;
$q_7 = s_2BBs_YR$ (SIM); $q_8 = s_2aas_NR$ (NÃO);
$q_9 = s_2bbs_NN$ (NÃO).

13.85 (*a*) $\langle 6\rangle = 1^7$; (*b*) $\langle m\rangle = 1^6B1B1^4B1^2$; (*c*) $\langle m\rangle = 1B1B1$; (*d*) não definido.

13.86 (*a*) $[E] = 7$; (*b*) $[E] = 2$; (*c*) $[E] = 14$.

13.87 Estratégia: apague os primeiros três 1s:

$q_1 = s_0 1Bs_1R$, $q_2 = s_1BBs_HN$ (pára), $q_3 = s_1 1Bs_2R$,
$q_4 = s_2BBs_HN$ (pára), $q_5 = s_2 1Bs_HN$.

13.88 Estratégia: apague o primeiro 1 e, após, todos os 1s depois de B:

$q_1 = s_0 1Bs_1R$, $q_2 = s_1 1 1s_1R$, $q_3 = s_1BBs_2R$,
$q_4 = s_2 1Bs_3R$, $q_5 = s_3 1Bs_3R$, $q_6 = s_3BBs_HN$ (pára).

Capítulo 14

Conjuntos Ordenados e Reticulados

14.1 INTRODUÇÃO

Ordem e relações de precedência aparecem em muitas ocasiões em matemática e ciência da computação. Este capítulo torna precisas essas noções. Definimos também um reticulado, que é um tipo particular de conjunto ordenado.

14.2 CONJUNTOS ORDENADOS

Suponha que R é uma relação em um conjunto S satisfazendo as três propriedades seguintes:

$[\mathbf{O}_1]$ (Reflexiva) para cada $a \in S$, temos aRa.

$[\mathbf{O}_2]$ (Anti-simétrica) se aRb e bRa, então $a = b$.

$[\mathbf{O}_3]$ (Transitiva) se aRb e bRc, então aRc.

Então, R é dita uma *ordem parcial* ou, simplesmente, uma *relação de ordem*, e diz-se que R define uma *ordenação parcial* de S. O conjunto S com a ordem parcial é dito um *conjunto parcialmente ordenado* ou, simplesmente, um conjunto ordenado. Escrevemos (S, R) quando queremos especificar a relação R.

A relação de ordem mais comum, conhecida como ordem usual, é a relação $\leq$ (lê-se "menor ou igual") nos inteiros positivos $\mathbf{N}$ ou, mais geralmente, em qualquer subconjunto dos números reais $\mathbf{R}$. Por esta razão, uma relação de ordem parcial é comumente denotada por $\preceq$; e

$$a \preceq b$$

é lido como "a precede b". Neste caso, escrevemos também:

$a \prec b$ significa $a \preceq b$ e $a \neq b$; lê-se "a precede b estritamente".

$b \succeq a$ significa $a \preceq b$; lê-se "b sucede a".

$b \succ a$ significa $a \prec b$; lê-se "b sucede a estritamente".

$\npreceq$, $\not\prec$, $\not\succeq$ e $\not\succ$ têm significado claro.

Quando não há possibilidade de ambigüidades, os símbolos $\leq$, $<$, $>$ e $\geq$ são freqüentemente usados no lugar de $\preceq$, $\prec$, $\succ$ e $\succeq$, respectivamente.

Exemplo 14.1

(*a*) Seja $\mathcal{S}$ uma coleção qualquer de conjuntos. A relação $\subseteq$ de inclusão de conjuntos é uma ordenação parcial de $\mathcal{S}$. Especificamente, $A \subseteq A$ para qualquer conjunto A; se $A \subseteq B$ e $B \subseteq A$, então $A = B$; se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.

(*b*) Considere o conjunto **N** de inteiros positivos. Dizemos que "*a* divide *b*" (escreve-se $a|b$) se existe um inteiro c tal que $ac = b$. Por exemplo, $2|4$, $3|12$, $7|21$ e assim por diante. Essa relação de divisibilidade é uma ordem parcial em **N**.

(*c*) A relação "|" de divisibilidade não é uma ordem parcial no conjunto **Z** dos inteiros. Especificamente, a relação não é anti-simétrica. Por exemplo, $2|-2$ e $-2|2$, mas $2 \neq -2$.

(*d*) Considere o conjunto **Z** dos inteiros. Defina aRb se existe um inteiro positivo r tal que $b = a^r$. Por exemplo, $2R8$ uma vez que $8 = 3^2$. Então, R é uma ordenação parcial de **Z**.

Ordem Dual

Seja $\precsim$ uma ordenação parcial de um conjunto S. A relação $\succsim$, isto é, a sucede b, também é uma ordenação parcial de S; ela é chamada de *ordem dual*. Observe que $a \precsim b$ se e somente se $b \succsim a$; logo, a ordem dual $\succsim$ é a inversa da relação $\precsim$, isto é, $\succsim = \precsim^{-1}$.

Subconjuntos Ordenados

Seja A um subconjunto de um conjunto ordenado S e suponha que $a, b \in A$. Defina $a \precsim b$ em A sempre que $a \precsim b$ em S. Define-se assim uma ordenação parcial de A chamada *ordem induzida* em A. O subconjunto a com a ordem induzida é dito um *subconjunto ordenado* de S. Todo subconjunto de um conjunto ordenado de S será tratado como subconjunto ordenado de S, a menos que afirmação em contrário seja feita ou esteja implícita.

Quasi-Ordem

Suponha que $\prec$ é uma relação em um conjunto S satisfazendo as duas propriedades seguintes:

$[\mathbf{Q}_1]$ (Não-reflexiva) para todo $a \in A$, $a \not\prec a$.

$[\mathbf{Q}_2]$ (Transitiva) se $a \prec b$ e $b \prec c$, então $a \prec c$.

Então, $\prec$ é chamada de uma *quasi-ordem* em S.

Existe uma íntima relação entre quasi-ordens e ordens parciais. Especificamente, se $\precsim$ é uma ordem parcial em um conjunto S e definimos que $a \prec b$ significa $a \precsim b$ mas $a \neq b$, então $\prec$ é uma quasi-ordem em S. Conversamente, se $\prec$ é uma quasi-ordem em um conjunto S e definimos que $a \precsim b$ significa $a \prec b$ ou $a = b$, então $\precsim$ é uma ordem parcial em S. Isto nos permite transitar entre uma ordem parcial e sua quasi-ordem correspondente de acordo com o que for mais conveniente.

Comparabilidade e Conjuntos Linearmente Ordenados

Suponha que a e b são elementos em um conjunto parcialmente ordenado S. Dizemos que a e b são *comparáveis* se

$$a \precsim b \qquad \text{ou} \qquad b \precsim a$$

isto é, se um deles precede o outro. Logo, a e b são *não-comparáveis*, denotado por

$$a \| b$$

se nenhuma das duas opções entre $a \precsim b$ e $b \precsim a$ ocorre.

A palavra parcial é usada na definição de um conjunto parcialmente ordenado S porque alguns dos elementos de S não são necessariamente comparáveis. Suponha, por outro lado, que todo par de elementos de S seja comparável. Neste caso, S é dito um conjunto *totalmente ordenado* ou *linearmente ordenado*, sendo chamado *cadeia*[†]. Ainda que um conjunto ordenado S não seja linearmente ordenado, é possível que um subconjunto A de S o seja. Claramente, todo subconjunto de um conjunto linearmente ordenado é linearmente ordenado.

[†] N. de T. No original, *chain*.

Exemplo 14.2

(*a*) Considere o conjunto **N** dos inteiros positivos ordenados pela divisibilidade. Então, 21 e 7 são comparáveis, já que 7|21. Por outro lado, 3 e 5 não são comparáveis, pois nem 3|5 nem 5|3. Logo, **N** não é linearmente ordenado pela divisibilidade. Observe que $A = \{2, 6, 12, 36\}$ é um subconjunto linearmente ordenado de **N**, pois 2|6, 6|12 e 12|36.

(*b*) O conjunto **N** dos inteiros positivos com a ordem usual $\leq$ (menor ou igual) é linearmente ordenado, portanto, todo subconjunto ordenado de **N** também é linearmente ordenado.

(*c*) O conjunto das partes de A, $P(A)$, onde A um conjunto com dois ou mais elementos, não é linearmente ordenado pela inclusão de conjuntos. Por exemplo, suponha que a e b pertencem a A. Então $\{a\}$ e $\{b\}$ são não-comparáveis. Observe que o conjunto vazio, $\emptyset$, $\{a\}$ e A formam um subconjunto linearmente ordenado de $P(A)$, pois $\emptyset \subseteq \{a\} \subseteq A$. De modo similar, $\emptyset$, $\{b\}$ e A formam um subconjunto linearmente ordenado de $P(A)$.

Conjuntos de Produto e Ordem

Existem várias maneiras de definir uma relação de ordem no produto cartesiano de conjuntos ordenados dados. Duas destas maneiras estão descritas a seguir.

(*a*) ***Ordem do produto***: suponha que S e T são conjuntos linearmente ordenados. Então, pode-se definir uma relação de ordem no produto $S \times T$, conhecida como *ordem do produto*, como:

$$(a, b) \precsim (a', b') \qquad \text{se} \qquad a \leq a' \text{ e } b \leq b'$$

(*b*) ***Ordem lexicográfica***: suponha que S e T são conjuntos linearmente ordenados. Então, pode-se definir uma relação de ordem no produto $S \times T$, conhecida como *ordem lexicográfica*, como:

$$(a, b) \prec (a', b') \qquad \text{se} \qquad a < b \qquad \text{ou se} \qquad a = a' \text{ e } b < b'$$

Note que a ordem lexicográfica também é linear.

Fecho de Kleene e Ordem

Seja A um alfabeto (não vazio) linearmente ordenado. Lembre que A^*, conhecido como o fecho de Kleene de A, consiste em todas as palavras w em A, e $|w|$ denota o comprimento de w. As relações seguintes são duas relações de ordem em A.

(*a*) ***Ordem alfabética (lexicográfica)***: o leitor é indubitavelmente familiarizado com a ordem alfabética de A^*. Isto é:

(i) $\lambda < w$, onde λ é a palavra vazia e w é qualquer palavra não vazia.

(ii) Suponha que $u = au'$ e $v = bv'$ são palavras não vazias distintas onde $a, b \in A$ e $u', v' \in A^*$. Então,

$$u \prec v \qquad \text{se } a < b \qquad \text{ou} \qquad \text{se } a = b \text{ mas } u' \prec v'$$

(*b*) ***Ordem comp-lex***: aqui, A^* é ordenado primeiramente pelo comprimento e depois alfabeticamente. Para quaisquer palavras distintas u, v em A^*,

$$u \prec v \qquad \text{se } |u| < |v| \qquad \text{ou se } |u| = |v|, \text{ mas } u \text{ precede } v \text{ alfabeticamente.}$$

Por exemplo, "tu" precede "nós" pois |tu| = 2, mas |nós| = 3. Entretanto "nó" precede "tu" pois, embora tenham o mesmo comprimento, "nó" precede "tu" na ordem alfabética. Essa ordem também é conhecida como *ordem de semigrupo livre*.

14.3 DIAGRAMAS DE HASSE DE CONJUNTOS PARCIALMENTE ORDENADOS

Seja S um conjunto parcialmente ordenado e suponha que a e b pertencem a S. Dizemos que a é um *predecessor imediato* de b ou que b é um *sucessor imediato* de a, escrevendo:

$$a \ll b$$

se $a < b$ mas nenhum elemento em S está entre a e b, isto é, não existe elemento c em S tal que $a < c < b$.

Suponha que S é um conjunto finito parcialmente ordenado. Então, a ordem em S é completamente determinada uma vez que se conheça todos os pares a, b em S tais que $a \ll b$, isto é, uma vez que a relação $\ll$ seja conhecida. Isto é conseqüência do fato de que $x < y$ se e somente se $x \ll y$ ou existem elementos $a_1, a_2, \ldots, a_m$ em S tais que

$$x \ll a_1 \ll a_2 \ll \cdots \ll a_m \ll y$$

O *diagrama de Hasse* de um conjunto finito parcialmente ordenado S é o grafo orientado cujos vértices são os elementos de S, e existe uma aresta orientada de a para b sempre que $a \ll b$ em S. (Em vez de desenhar uma seta de a para b, colocamos, às vezes, b acima de a, e desenhamos uma linha entre eles. Fica então entendido que movimento ascendente indica sucessão.) No diagrama assim construído, existe um caminho orientado do vértice x para o vértice y se e somente se $x < y$. Além disso, não podem ocorrer ciclos (orientados) no diagrama de S já que a relação de ordem é anti-simétrica.

O diagrama de Hasse de um conjunto finito parcialmente ordenado é uma representação de S; portanto, é muito útil na descrição dos tipos de elementos de S. Às vezes, definimos um conjunto finito parcialmente ordenado com a simples apresentação do seu diagrama de Hasse. Observamos que o diagrama de Hasse de um conjunto finito parcialmente ordenado não precisa ser conexo.

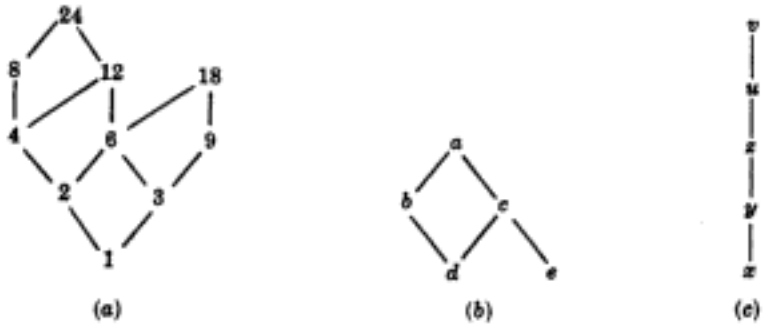
Observação: O diagrama de Hasse de um conjunto finito parcialmente ordenado S é um grafo acíclico orientado, estudado na Seção 9.9. A investigação feita aqui independe de estudo prévio. Aqui, pensamos prioritariamente em termos de "menor que" ou "maior que" em detrimento de relações de adjacências orientadas. Conseqüentemente, ocorrerão algumas redundâncias de conteúdo.

Exemplo 14.3

(*a*) Seja $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$ ordenado pela relação "x divide y". O diagrama de A é mostrado na Figura 14-1(*a*). (Ao contrário do caso de árvores com raízes, a direção da linha em um diagrama de um conjunto parcialmente ordenado é sempre ascendente.)

(*b*) Seja $B = \{a, b, c, d, e\}$. O diagrama da Figura 14-1(*b*) define uma ordem parcial em B de modo natural. Isto é, $d \le b$, $d \le a$, $e \le c$, e assim por diante.

(*c*) O diagrama de um conjunto finito parcialmente ordenado, i.e., uma cadeia finita, consiste em apenas um caminho. Por exemplo, a Figura 14-1(*c*) mostra o diagrama de uma cadeia com cinco elementos.



(*a*) (*b*) (*c*)

Fig. 14-1

Exemplo 14.4 Uma *partição* de um inteiro positivo m é um conjunto de inteiros positivos cuja soma é m. Por exemplo, existem sete partições de $m = 5$ como indicamos a seguir.

$$5, \quad 3-2, \quad 2-2-1, \quad 1-1-1-1-1, \quad 4-1, \quad 3-1-1, \quad 2-1-1-1$$

Ordenamos as partições de um inteiro m do modo descrito a seguir. A partição P_1 precede a partição P_2 se os inteiros em P_1 puderem ser acrescentados para obter os elementos de P_2, ou, equivalentemente, se os inteiros em P_2 puderem ser posteriormente subdivididos para obter os inteiros em P_1. Por exemplo,

$$2-2-1 \qquad \text{precede} \qquad 3-2$$

pois $2 + 1 = 3$. Por outro lado, $3 - 1 - 1$ e $2 - 2 - 1$ são não-comparáveis.

A Figura 14-2 mostra o diagrama de Hasse das partições de $m = 5$.

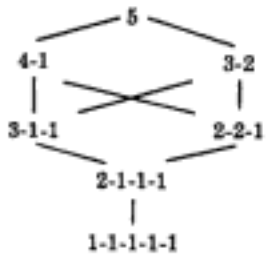


Fig. 14-1

Elementos Minimal e Maximal, Primeiro e Último

Seja S um conjunto parcialmente ordenado. Um elemento $a \in S$ é dito um elemento *minimal* se nenhum outro elemento de S precede estritamente (é menor que) a. Analogamente, um elemento $b \in S$ é dito um elemento *maximal* se nenhum elemento de S sucede estritamente (é maior que) b. Falando sob o ponto de vista gráfico, a é minimal se nenhuma aresta incide (inferiormente) em a, e b é um elemento maximal se nenhuma aresta deixa b (em direção ascendente). Notamos que S pode ter mais de um elemento minimal e mais de um elemento maximal.

Se S é infinito, é possível que S não tenha elemento maximal ou elemento minimal. Por exemplo, o conjunto $\mathbf{Z}$ dos inteiros com a ordem usual $\leq$ não tem nem elemento minimal nem elemento maximal. Por outro lado, se S é finito, então S deve ter pelo menos um elemento maximal e pelo menos um elemento minimal.

Um elemento a em S é dito um *primeiro* elemento se

$$a \precsim x$$

para todo elemento x em S, isto é, se a precede qualquer outro elemento em S. Analogamente, um elemento b em S é dito um *último* elemento se

$$y \precsim b$$

para todo elemento y em S, isto é, se b sucede qualquer outro elemento em S. Notamos que S tem no máximo um primeiro elemento, que deve ser um elemento minimal, e S pode ter, no máximo, um último elemento, que deve ser maximal. Genericamente, S pode não ter nem primeiro nem último elemento, mesmo se S for finito.

Exemplo 14.5

(*a*) Considere os três conjuntos parcialmente ordenados no Exemplo 14-3 cujo diagrama de Hasse aparece na Figura 14-1.

(i) A tem dois elementos maximais, 18 e 24, e nenhum é um último elemento. A tem apenas um elemento minimal, 1, que também é um primeiro elemento.

(ii) B tem dois elementos minimais, d e e, e nenhum é um primeiro elemento. B só tem um elemento maximal, a, que também é um último elemento.

(iii) A cadeia tem um elemento minimal, x, que é um primeiro elemento, e um elemento maximal v, que é um último elemento.

(*b*) Seja A um conjunto qualquer não vazio e seja $P(A)$ o conjunto das partes de A com a relação de inclusão de conjuntos. O conjunto vazio, $\emptyset$, é um primeiro elemento de $P(A)$, pois, para qualquer conjunto X, temos $\emptyset \subseteq X$. Além disso, A é um último elemento de $P(A)$ já que todo elemento Y de $P(A)$ é, por definição, um subconjunto de A, isto é, $Y \subseteq A$.

14.4 ENUMERAÇÃO CONSISTENTE

Suponha que S é um conjunto finito parcialmente ordenado. Freqüentemente, queremos associar inteiros positivos aos elementos de S de tal maneira que a ordem seja preservada. Isto é, procuramos uma função $f: S \to \mathbf{N}$ tal que, se $a \prec b$, então $f(a) < f(b)$. Uma função como esta é conhecida como *enumeração consistente* de S. O fato de isto sempre poder ser feito é o conteúdo do próximo teorema.

Teorema 14-1: existe uma enumeração consistente para todo conjunto finito parcialmente ordenado.

Mostramos esse teorema no Problema 14.15. De fato, provamos que, se S tem n elementos, existe uma enumeração consistente f: $S \to \{1, 2, \ldots, n\}$.

Enfatizamos que uma tal enumeração não precisa ser única. Por exemplo, apresentamos a seguir duas enumerações deste tipo para o conjunto parcialmente ordenado da Figura 14-1(b):

(i) $f(d) = 1,\ f(e) = 2,\ f(b) = 3,\ f(c) = 4,\ f(a) = 5$

(ii) $g(e) = 1,\ g(d) = 2,\ g(c) = 3,\ g(b) = 4,\ g(a) = 5$

Entretanto, a cadeia da Figura 14-1(c) admite apenas uma enumeração consistente se o conjunto for mapeado em $\{1, 2, 3, 4, 5\}$. Especificamente, é preciso atribuir:

$$h(x) = 1, \qquad h(y) = 2, \qquad h(z) = 3, \qquad h(u) = 4, \qquad h(v) = 5$$

14.5 *SUPREMUM* E *INFIMUM*

Seja A um subconjunto de um conjunto parcialmente ordenado S. Um elemento M em S é dito um *limite superior* de A se M sucede todo elemento de A, i.e., se para todo x em A, temos

$$x \precsim M$$

Se um limite superior de A precede qualquer outro limite superior de A, então ele é dito o *supremum* de A e é denotado por

$$\sup(A)$$

Também escrevemos $(a_1, \ldots, a_n)$ no lugar de sup(A) se A consiste nos elementos $a_1, \ldots, a_n$. Enfatizamos que pode existir, no máximo, um sup(A); entretanto, sup(A) pode não existir.

Analogamente, um elemento M em um conjunto parcialmente ordenado S é dito um *limite inferior* de A se M precede todo elemento de A, i.e., se para todo y em A, temos

$$m \precsim y$$

Se um limite inferior de A precede qualquer outro limite inferior de A, então ele é dito o *infimum* de A e é denotado por

$$\inf(A) \qquad \text{ou} \qquad \inf(a_1, \ldots, a_n)$$

se A consiste nos elementos $a_1, \ldots, a_n$. Pode existir, no máximo, um inf(A), embora inf(A) possa não existir.

Alguns textos usam o termo *menor limite superior* em vez de *supremum* e escrevem mls(A)[†] no lugar de sup(A), e usam *maior limite inferior* escrevendo mli(A)[††] em vez de inf(A).

Se A tem um limite superior, dizemos que A é *superiormente limitado* e, se A tem um limite inferior, dizemos que A é *inferiormente limitado*. Em particular, A é *limitado* se tem limites inferior e superior.

Exemplo 14.6

(*a*) Seja $S = \{a, b, c, d, e, f\}$, ordenado como na Figura 14-3(a), e seja $A = \{b, c, d\}$. Os limites superiores de A são e e f, já que apenas e e f sucedem todo elemento de A. Os limites inferiores de A são a e b, já que apenas a e b precedem todo elemento de A. Note que e e f são não-comparáveis; portanto, não existe sup(A). Entretanto, b também sucede a. Portanto, inf(A) = b.

(*b*) Seja $S = \{1, 2, 3\ldots, 8\}$ ordenado como na Figura 14-3(b), e seja $A = \{4, 5, 7\}$. Os limites superiores de A são 1, 2 e 3, e o único limite inferior é 8. Note que 7 não é um limite inferior, pois 7 não precede 4. Neste caso, sup(A) = 3, pois 3 precede os outros limites superiores 1 e 2. Note que inf(A) = 8, já que 8 é o único limite inferior.

[†] N. de T. No original, lub(A), referente a *least upper bound*.

[††] N. de T. No original, glb(A), referente a *greatest lower bound*.

(*a*) (*b*)

Fig. 14-3

Genericamente, sup(a, b) e inf(a, b) não precisam existir para todo par de elementos a e b em um conjunto S parcialmente ordenado[†]. Apresentamos agora dois exemplos de conjuntos parcialmente ordenados onde sup(a, b) e inf(a, b) existem para todo a, b no conjunto.

Exemplo 14.7

(*a*) Considere o conjunto **N** de inteiros positivos ordenados por divisibilidade. O *máximo divisor comum* de a e b em **N**, denotado por

$$\text{mdc}\ (a, b)$$

é o maior inteiro que divide a e b. O *mínimo múltiplo comum* de a e b, denotado por

$$\text{mmc}\ (a, b)$$

é o menor inteiro divisível por ambos, a e b.

Um teorema importante da teoria dos números afirma que todo divisor comum de a e b divide mdc(a, b). Pode-se mostrar também que mmc (a, b) divide todo múltiplo de a e b. Logo,

$$\text{mdc}(a,b) = \inf(a,b) \qquad \text{e} \qquad \text{mmc}(a,b) = \sup(a,b)$$

Em outras palavras, inf(a, b) e sup(a, b) existem para todo par de elementos de **N** ordenado por divisibilidade.

(*b*) Para todo inteiro positivo m, denotaremos por $\mathbf{D}_m$ o conjunto de todos os divisores de m ordenados por divisibilidade. O diagrama de Hasse de

$$\mathbf{D}_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

aparece na Figura 14-4. Novamente, inf(a, b) = mdc(a, b) e sup(a, b) = mmc (a, b) existem para qualquer par a, b em $\mathbf{D}_m$.

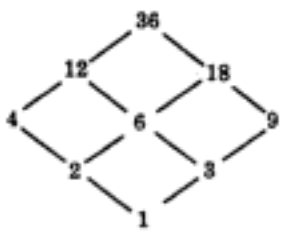


Fig. 14-4

14.6 CONJUNTOS ORDENADOS ISOMORFOS (SIMILARES)

Suponha que X e Y são conjuntos parcialmente ordenados. Uma função injetora f: $X \to Y$ é dita um *mapeamento de similaridade* de X em Y se f preserva a relação de ordem, isto é, se valem as seguintes duas condições para todo par a, a' em X

(1) Se $a \precsim a'$, então $f(a) \precsim f(a')$.

(2) Se $a \parallel a'$ (não-comparável), então $f(a) \parallel f(b)$.

Conseqüentemente, se A e B são linearmente ordenados, apenas a condição (1) é necessária para que f seja um mapeamento de similaridade.

[†] N. de T. Embora os conceitos de inf e sup só tenham sido definidos para conjuntos, aqui o autor os utiliza para um par de elementos. A tradução é fiel ao original.

Dois conjuntos X e Y são ditos *isomorfos* ou *similares*, o que se denota por

$$X \simeq Y$$

se existe uma correspondência bijetora f: $X \to Y$ que preserva a relação de ordem, i.e., que é um mapeamento de similaridade.

Exemplo 14.8 Suponha que $X = \{1, 2, 6, 8, 12\}$ é ordenado pela divisibilidade, e suponha que $Y = \{a, b, c, d, e\}$ é isomorfo a X; por exemplo, a função seguinte é um mapeamento de similaridade de X sobre Y:

$$f = \{(1, e),\ (2, d),\ (6, b),\ (8, c),\ (12, a)\}$$

Desenhe o diagrama de Hasse de Y.

O mapeamento de similaridade preserva a ordem do conjunto inicial X e é injetor e sobrejetor. Logo, o mapeamento pode ser visto como apenas uma renomeação dos vértices do diagrama de Hasse do conjunto inicial X. Os diagramas de Hasse de ambos, X e Y, aparecem na Figura 14-5.

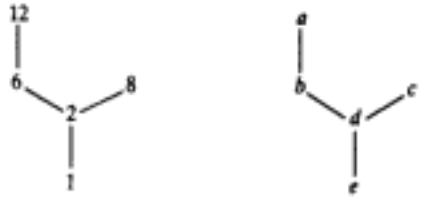


Fig. 14-5

14.7 CONJUNTOS BEM-ORDENADOS

Iniciamos com uma definição.

Definição: Um conjunto ordenado S é dito *bem-ordenado* se todo subconjunto de S tem um primeiro elemento.

O exemplo clássico de um conjunto bem-ordenado é o conjunto $\mathbf{N}$ dos inteiros positivos com a ordem usual $\leq$. Os seguintes fatos são conseqüências imediatas da definição.

(1) Um conjunto bem-ordenado é linearmente ordenado. De fato, se $a, b \in S$, então $\{a, b\}$ tem um primeiro elemento; logo, a e b são comparáveis.

(2) Todo subconjunto de um conjunto bem-ordenado é bem-ordenado.

(3) Se X é bem-ordenado e Y é isomorfo a X, então Y é bem-ordenado.

(4) Todos os conjuntos finitos linearmente ordenados com o mesmo número n de elementos são bem-ordenados, e todos são isomorfos entre si. De fato, todos são isomorfos a $\{1, 2, \ldots n\}$ com a ordem usual $\leq$.

(5) Todo elemento $a \in S$, que não é um último elemento, tem um sucessor imediato. De fato, seja $M(a)$ o conjunto de elementos que sucedem a estritamente; o primeiro elemento de $M(a)$ é o sucessor imediato de a.

Exemplo 14.9

(*a*) O conjunto $\mathbf{Z}$ dos inteiros com a ordem usual $\leq$ é linearmente ordenado, e todo elemento tem um sucessor imediato e um predecessor imediato, mas $\mathbf{Z}$ não é bem-ordenado. Por exemplo, o próprio $\mathbf{Z}$ não tem um primeiro elemento. Entretanto, qualquer subconjunto de $\mathbf{Z}$ inferiormente limitado é bem-ordenado.

(b) O conjunto $\mathbf{Q}$ dos números racionais com a ordem usual $\leq$ é linearmente ordenado, mas nenhum elemento em $\mathbf{Q}$ tem um sucessor imediato ou um predecessor imediato. Pois se $a, b \in Q$, digamos $a < b$ então $(a + b)/2 \in \mathbf{Q}$ e

$$a < \frac{a+b}{2} < b$$

(*c*) Considere os conjuntos bem-ordenados disjuntos

$$A = \{1, 3, 5, \ldots\} \qquad \text{e} \qquad B = \{2, 4, 6, \ldots\}$$

Então, o seguinte conjunto ordenado

$$S = \{A; B\} = \{1, 3, 5, \ldots; 2, 4, 6, \ldots\}$$

é bem-ordenado. Além do primeiro elemento 1, o elemento 2 não tem predecessor imediato.

Notação: Aqui e no texto subseqüente, se A, B,... são conjuntos disjuntos, $\{A; B;\ldots\}$ significa o conjunto $A \cup B \cup \ldots$ ordenado por posição, da esquerda para direita; isto é, os elementos no mesmo conjunto mantêm sua ordem, e qualquer elemento de um conjunto à esquerda precede qualquer elemento de um conjunto à sua direita. Assim todo elemento em A precede todo elemento em B, e assim por diante.

Indução Transfinita

Primeiramente reafirmamos o princípio de indução matemática. (Veja as Seções 1.10 e 1.13.)

Princípio da indução matemática: seja A um subconjunto do conjunto **N** de inteiros positivos com as seguintes duas propriedades:

(i) $1 \in A$.

(ii) Se $n \in A$, então $n + 1 \in A$.

Então, $A = \mathbf{N}$.

O princípio acima é um dos axiomas de Peano para os números naturais (inteiros positivos) **N**. Existe uma outra forma cujo uso é, às vezes, mais conveniente.

Princípio da indução matemática (segunda forma): seja A um subconjunto de **N** com as duas propriedades seguintes:

(i) $1 \in A$.

(ii) Se k pertence a A para $1 \leq k < n$, então $n \in A$.

Então, $A = \mathbf{N}$.

A segunda forma da indução é equivalente ao fato de **N** ser bem-ordenado (Teorema 11-6). Na verdade, existe uma afirmação, em um certo sentido similar, que é verdade para todo conjunto bem-ordenado.

Princípio da indução transfinita: seja A é um subconjunto de um conjunto bem-ordenado S com as seguintes duas propriedades:

(i) $a_0 \in A$.

(ii) Se $s(a) \subseteq A$, então $a \in A$.

Então, $A = S$.

Neste caso, a_0 é o primeiro elemento de S e $s(a)$, denominado *segmento inicial* de a, é definido como o conjunto de todos os elementos de S que precedem a estritamente.

O Axioma da Escolha e O Teorema da Boa Ordenação

Seja $\{A_i : i \in I\}$ uma coleção de conjuntos disjuntos não vazios. Assumimos que $A_i \subseteq X$. Uma função $f: \{A_i\} \to X$ é dita uma *função de escolha* se $f(A_i) = a_i \in A_i$. Em outras palavras, f "escolhe" um ponto $a_i \in A_i$ para cada A_i.

O axioma da escolha está nos fundamentos da matemática e, em particular, na teoria dos conjuntos. Esse axioma, aparentemente "ingênuo", enunciado a seguir, tem como conseqüência alguns dos mais importantes e poderosos resultados da matemática.

Axioma da escolha: existe uma função de escolha para qualquer coleção não vazia de conjuntos disjuntos não vazios.

Uma das conseqüências do axioma da escolha é o teorema seguinte, atribuído a Zermelo.

Teorema da boa ordenação: todo conjunto S pode ser bem-ordenado.

A prova deste teorema está além dos objetivos deste texto. Além disso, como todas as nossas estruturas são finitas e enumeráveis, não precisaremos usar este teorema. A indução matemática comum é suficiente.

14.8 RETICULADOS

Seja L um conjunto não vazio fechado sob duas operações binárias chamadas *conjunção* e *disjunção*[†], denotadas, respectivamente, por $\wedge$ e $\vee$. L é denominado um *reticulado* se valem os axiomas seguintes, onde a, b e c são elementos de L.

$[\mathbf{L}_1]$ Lei da comutatividade:

$(1a)$ $a \wedge b = b \wedge a$ $\qquad$ $(1b)$ $a \vee b = b \vee a$

$[\mathbf{L}_2]$ Lei da associatividade:

$(2a)$ $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ $\qquad$ $(2b)$ $(a \vee b) \vee c = a \vee (b \vee c)$

$[\mathbf{L}_3]$ Lei da absorção:

$(3a)$ $a \wedge (a \vee b) = a$ $\qquad$ $(3b)$ $a \vee (a \wedge b) = a$

Às vezes, denotaremos o reticúlado por $(L, \wedge, \vee)$ quando quisermos explicitar as operações envolvidas.

Dualidade e Lei de Idempotência

A declaração dual de qualquer declaração em um reticulado $(L, \wedge, \vee)$ é definida como sendo a declaração obtida pela troca de $\wedge$ por $\vee$. Por exemplo, a dual de

$$a \wedge (b \vee a) = a \vee a \qquad \text{é} \qquad a \vee (b \wedge a) = a \wedge a$$

Note que o dual de cada axioma em um reticulado também é um axioma. Conseqüentemente, vale o princípio da dualidade; isto é:

Teorema 14-2: (**Princípio da dualidade**) o dual de qualquer teorema em um reticulado também é um teorema.

Isso é uma conseqüência do fato de que o teorema dual pode ser demonstrado usando o dual de cada passo na demonstração do teorema original.

Uma propriedade importante de reticulados segue diretamente das leis de absorção.

Teorema 14-3: (**Lei de idempotência**) (i) $a \wedge a = a$, (ii) $a \vee a = a$

A demonstração requer apenas duas linhas:

$$\begin{aligned} a \wedge a &= a \wedge (a \vee (a \wedge b)) && \text{(usando(3}b\text{))} \\ &= a && \text{(usando(3a))} \end{aligned}$$

A demonstração de (ii) segue do princípio da dualidade acima (ou pode ser feita de modo similar).

Reticulados e Ordem

Dado um reticulado L, podemos definir uma ordem parcial em L como a seguir:

$$a \preceq b \qquad \text{se} \qquad a \wedge b = a$$

Analogamente, poderíamos definir

$$a \succeq b \qquad \text{se} \qquad a \vee b = b$$

Enunciamos estes resultados como um teorema.

Teorema 14-4: seja L um reticulado. Então,

[†] N. de T. No original, *meet* e *join*, respectivamente.

Hidden page

14.9 RETICULADOS LIMITADOS

Diz-se que um reticulado tem um *limite inferior* 0 se, para todo elemento x em L, vale $0 \precsim x$. Analogamente, diz-se que L tem um *limite superior* I se, para todo x em L, temos $x \precsim I$. Dizemos que L é *limitado* se L tem ambos, limite inferior 0 e limite superior I. Em um tal reticulado, valem as identidades

$$a \vee I = I, \qquad a \wedge I = a, \qquad a \vee 0 = a, \qquad a \wedge 0 = 0$$

para todo elemento a em L.

Os inteiros não negativos com a ordem usual

$$0 < 1 < 2 < 3 < 4 < \dots$$

têm 0 como limite inferior, mas não têm limite superior. Por outro lado, o reticulado $P(U)$ de todos os subconjuntos do conjunto universo U é um reticulado limitado tendo U como limite superior e o conjunto vazio, $\varnothing$, como limite inferior.

Suponha que $L = \{a_1, a_2, \dots, a_n\}$ é um reticulado finito. Então,

$$a_1 \vee a_2 \vee \cdots \vee a_n \qquad \text{e} \qquad a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

são limites superior e inferior, respectivamente, para L. Assim temos

Teorema 14-6: todo reticulado finito L é limitado.

14.10 RETICULADOS DISTRIBUTIVOS

Um reticulado L é dito *distributivo* se, para quaisquer elementos a, b e c em L, temos o seguinte:

$[\mathbf{L}_4]$ Lei da distributividade

$$(4a)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad (4b)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Caso contrário, L é dito *não distributivo*. Notamos que, pelo princípio da dualidade, a condição $(4a)$ vale se e somente se $(4b)$ vale.

A Figura 14-7(a) mostra um reticulado não distributivo, pois

$$a \vee (b \wedge c) = a \vee 0 = a \qquad \text{mas} \qquad (a \vee b) \wedge (a \vee c) = I \wedge c = c$$

A Figura 14-7(b) também contém um reticulado não distributivo. De fato, temos a caracterização seguinte para reticulados não-distributivos.

Teorema 14-7: um reticulado L é não distributivo se e somente se contém um sub-reticulado isomorfo à Figura 14-7(a) ou (b).

A prova deste teorema está além dos objetivos deste texto.

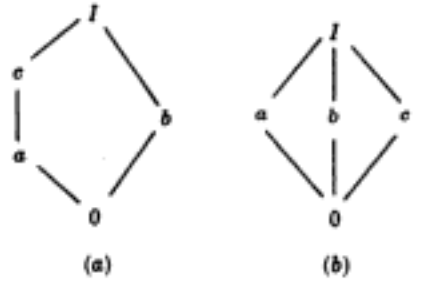


Fig. 14-7

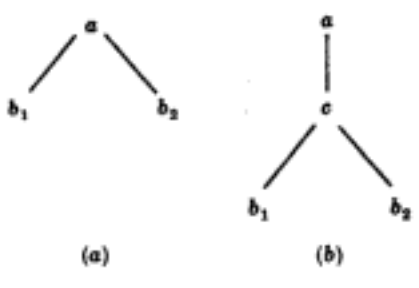


Fig. 14-8

Elementos Irredutíveis por Disjunção e Átomos

Seja L um reticulado com limite inferior 0. Um elemento a em L é dito *irredutível por disjunção* se $a = x \vee y$ implica em $a = x$ ou $a = y$. (Números primos sob multiplicação têm esta propriedade, i.e., se $p = ab$, então $p = a$ ou $p = b$ onde p é primo.) Claramente, 0 é irredutível por disjunção. Se a tem pelo menos dois predecessores imediatos, digamos b_1 e b_2, como na Figura 14-8(a), então $a = b_1 \vee b_2$ e, logo, a não é irredutível por disjunção. Por outro lado, se a tem um único predecessor imediato c, então $a \neq \sup(b_1, b_2) = b_1 \vee b_2$ para quaisquer outros elementos b_1 e b_2, porque c ficará entre os bs e a como na Figura 14-8(b). Em outras palavras, $a \neq 0$ é irredutível por disjunção se e somente se a tem um único predecessor imediato. Os elementos que sucedem 0 imediatamente, chamados de *átomos*, são irredutíveis por disjunção. Entretanto, reticulados podem ter outros elementos irredutíveis por disjunção. Por exemplo, o elemento c da Figura 14-7(a) não é um átomo mas é irredutível por disjunção, pois a é seu único predecessor imediato.

Se um elemento a em um reticulado finito L não é irredutível por disjunção, podemos escrever $a = b_1 \vee b_2$. Então, podemos escrever b_1 e b_2 como a disjunção de outros elementos se eles não são irredutíveis por disjunção, e assim por diante. Como L é finito, temos finalmente

$$a = d_1 \vee d_2 \vee \cdots \vee d_n$$

onde os ds são irredutíveis por disjunção. Se d_i precede d_j, então $d_i \vee d_j = d_j$; portanto, podemos deletar d_i da expressão. Em outras palavras, podemos assumir que os ds são *não-redundantes*, i.e., um d não pode preceder outro d. Enfatizamos que uma tal expressão não precisa ser única, por exemplo, $I = a \vee b$ e $I = b \vee c$ em ambos os reticulados da Figura 14-7. Agora, enunciamos o teorema principal desta seção (demonstrado no Problema 14.38).

Teorema 14-8: seja L um reticulado finto distributivo. Então, todo a em L pode ser escrito de maneira única (exceto pela ordem) como a disjunção de elementos não-redundantes irredutíveis por disjunção.

Na verdade, este teorema pode ser generalizado para reticulados de comprimento finito, i.e., em que todos os subconjuntos linearmente ordenados são finitos. (O Problema 14-33 mostra um reticulado infinito de comprimento finito.)

14.11 COMPLEMENTOS E RETICULADOS COMPLEMENTADOS

Seja L um reticulado limitado com limite inferior 0 e limite superior I. Seja a um elemento de L. Um elemento x em L é dito um *complemento* de a se

$$a \vee x = I \qquad \text{e} \qquad a \wedge x = 0$$

Complementos não precisam existir e não precisam ser únicos. Por exemplo, os elementos a e c são ambos complementos de b na Figura 14-7(a). Além disso, os elementos y, z e u na cadeia da Figura 14-1 não têm complementos. Temos o resultado a seguir.

Teorema 14-9: seja L um reticulado limitado distributivo. Os complementos são únicos, se existirem.

Demonstração: Suponha que x e y são complementos de um elemento qualquer em L. Então,

$$a \vee x = I, \qquad a \vee y = I, \qquad a \wedge x = 0, \qquad a \wedge y = 0$$

Usando distributividade,

$$x = x \vee 0 = x \vee (a \wedge y) = (x \vee a) \wedge (x \vee y) = I \wedge (x \vee y) = x \vee y$$

Similarmente,

$$y = y \vee 0 = y \vee (a \wedge x) = (y \vee a) \wedge (y \vee x) = I \wedge (y \vee x) = y \vee x$$

Logo,

$$x = x \vee y = y \vee x = y$$

E o teorema fica provado.

Reticulados Complementados

Um reticulado L é dito *complementado* se L é limitado e todo elemento de L tem um complemento. A Figura 14-7(b) mostra um reticulado complementado onde os complementos não são únicos. Por outro lado, o reticulado $P(U)$ de todos os subconjuntos do conjunto universo U é complementado, e cada subconjunto A de U tem o único complemento $A^c = U \backslash A$.

Teorema 14-10: seja L um reticulado complementado com complementos únicos. Então, os elementos irredutíveis por disjunção de L, diferentes de 0, são seus átomos.

Combinando este teorema e os Teoremas 14-8 e 14-9, obtemos um resultado importante.

Teorema 14-11: seja L um reticulado finito complementado. Então, todo elemento a de L é uma disjunção de um único conjunto de átomos.

Observação: Alguns textos definem um reticulado L como sendo complementado se cada a em L tem um complemento único. Neste caso, o Teorema 14-10 tem enunciado distinto.

Problemas Resolvidos

Conjuntos Ordenados e Subconjuntos

14.1 Suponha que o conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de inteiros positivos esteja ordenado por divisibilidade. Insira o símbolo correto, $\prec$, $\succ$ ou $\|$ (não-comparável) entre cada par de números.

(a) 2 ____ 8; (b) 18 ____ 24; (c) 9 ____ 3; (d) 5 ____ 15.

(a) Como 2 divide 8, 2 precede 8, i.e., $2 \prec 8$.

(b) 18 não divide 24 e 24 não divide 18; portanto, $18 \| 24$

(c) Como 9 é divisível por 3, $9 \succ 3$.

(d) Como 5 divide 15, $5 \prec 15$.

14.2 Seja $\mathbf{N} = \{1, 2, 3, \ldots\}$ ordenado por divisibilidade. Decida se cada um dos subconjuntos de $\mathbf{N}$ é linearmente (totalmente) ordenado.

(a) $\{24, 2, 6\}$ (c) $\mathbf{N} = \{1, 2, 3, \ldots\}$ (e) $\{7\}$

(b) $\{3, 15, 5\}$ (d) $\{2, 8, 32, 4\}$ (f) $\{15, 5, 30\}$

(a) Como 2 divide 6 que divide 24, o conjunto é linearmente ordenado.

(b) Como 2 e 5 não são comparáveis, o conjunto não é linearmente ordenado.

(c) Como 2 e 3 não são comparáveis, o conjunto não é linearmente ordenado.

(d) O conjunto é linearmente ordenado, pois $2 \prec 4 \prec 8 \prec 32$.

(e) Qualquer conjunto com um único elemento é linearmente ordenado.

(f) Como 5 divide 15 que divide 30, o conjunto é linearmente ordenado.

14.3 Seja $A = \{1, 2, 3, 4, 5\}$ ordenado pelo diagrama de Hasse da Figura 14-9. Insira o símbolo correto $\prec$, $\succ$ ou $\|$ (não-comparável) entre cada par de elementos.

(a) 1 ____ 5; (b) 2 ____ 3; (c) 4 ____ 1; (d) 3 ____ 4.

(a) Como existe um caminho (arestas para cima) de 5 para 3 para 1, 5 precede 1; portanto, $1 \succ 5$.

(b) Não existe caminho de 2 para 3 ou vice-versa; portanto, $2 \| 3$.

(c) Existe um caminho de 4 para 2 para 1; logo, $4 \prec 1$.

(d) Nem $3 \prec 4$ nem $4 \succ 3$; logo, $3 \| 4$.

Fig. 14-9

14.4 Considere o conjunto ordenado A da Figura 14-9.

(*a*) Ache os elementos minimal e maximal de A.

(*b*) A tem um primeiro ou um último elemento?

(*a*) Nenhum elemento precede estritamente 4 ou 5; logo, 4 e 5 são elementos minimais de A. Nenhum elemento sucede estritamente 1; portanto, 1 é um elemento maximal de A.

(*b*) A não tem primeiro elemento. Embora 4 e 5 sejam elementos minimais de A, nenhum dos dois precede o outro. Entretanto, 1 é um último elemento de A, já que 1 sucede todo elemento de A.

14.5 Considere o conjunto ordenado A da Figura 14-9. Seja $L(A)$ a coleção de todos os subconjuntos de A linearmente ordenados com dois ou mais elementos. Ordene $L(A)$ pela inclusão de conjuntos. Desenhe o diagrama de Hasse de $L(A)$.

Os elementos de $L(A)$ são:

$$\{1,2,4\},\quad \{1,2,5\},\quad \{1,3,5\}\quad \{1,2\},\quad \{1,4\},\quad \{1,3\},\quad \{1,5\},\quad \{2,4\},\quad \{2,5\},\quad \{3,5\}$$

(Note que $\{2,5\}$ e $\{3,4\}$ não são linearmente ordenados.) O diagrama de $L(A)$ aparece na Figura 14-10.

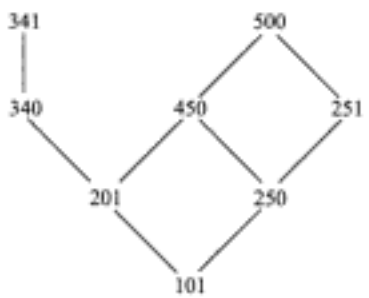
Fig. 14-10

14.6 Em uma escola, pré-requisitos são um exemplo familiar de ordem parcial dos cursos oferecidos. Dizemos que $A \ll B$ se o curso A é um pré-requisito para um curso B. Considere os cursos de matemática e seus pré-requisitos dados na Figura 14-11(*a*). Desenhe o diagrama de Hasse da ordem parcial destes cursos.

Mat 101 deve ficar no topo do diagrama, pois é o único curso sem pré-requisitos. Como Mat 201 e Mat 250 requerem apenas Mat 101, temos Mat 101 $\ll$ Mat 201 e Mat 101 $\ll$ Mat 250; portanto, desenhe uma linha saindo de Mat 101 indo em direção ascendente para Mat 201, e uma de Mat 101 para Mat 250. Continuando este processo, obtemos o diagrama de Hasse na Fig 14-11(*b*).

Curso	Pré-requisitos
Mat 101	Nenhum
Mat 201	Mat 101
Mat 250	Mat 101
Mat 251	Mat 250
Mat 340	Mat 201
Mat 341	Mat 340
Mat 450	Mat 201, Mat 250
Mat 500	Mat 450, Mat 251

(*a*)



(*b*)

Fig. 14-11

14.7 Considere o conjunto ordenado C das disciplinas de matemática da Figura 14-11.

(*a*) Determine todos os elementos maximais e minimais de C.

(*b*) C tem um primeiro ou último elemento?

(*a*) Nenhum elemento precede estritamente Mat 101 e, assim, Mat 101 é um elemento minimal de C. Nenhum elemento sucede estritamente Mat 341 ou Mat 500, então cada um deles é um elemento maximal de C.

(*b*) Mat 101 é um primeiro elemento de C, já que precede qualquer outro elemento em C. Entretanto, C não tem um último elemento. Embora Mat 341 e Mat 500 sejam elementos maximais, nenhum é um último elemento, já que nenhum dos dois precede o outro.

14.8 Considere o conjunto $\mathbf{N} = \{1, 2, 3, \ldots\}$ de inteiros positivos. Cada número em $\mathbf{N}$ pode ser escrito de maneira única como um produto de potências não negativas de 2, vezes um número ímpar. Suponha que a e a' são inteiros positivos tais que

$$a = 2^r(2s + 1) \qquad \text{e} \qquad a' = 2^{r'}(2s' + 1)$$

onde r e s são inteiros não negativos. Definimos:

$$a \prec a' \quad \text{se } r < r' \quad \text{ou se} \quad r = r' \text{ mas } s < s'$$

Insira o símbolo correto, $\prec$ ou $\succ$, entre cada um dos seguintes pares de números:

(*a*) 5 ____ 14; (*b*) 6 ____ 9; (*c*) 3 ____ 20; (*d*) 14 ____ 21.

Os elementos de $\mathbf{N}$ podem ser listados como na Figura 14-12. A primeira linha consiste nos números ímpares, e a segunda linha em 2 vezes os números ímpares, a terceira linha em $2^2 = 4$ vezes os números ímpares e assim por diante. Então, $a \prec a'$ se a for uma linha mais alta do que a', ou se a e a' estiverem na mesma linha mas a vier antes de a' na linha. Logo,

(*a*) $5 \prec 14$; (*b*) $6 \succ 9$; (*c*) $3 \succ 20$; (*d*) $14 \succ 21$.

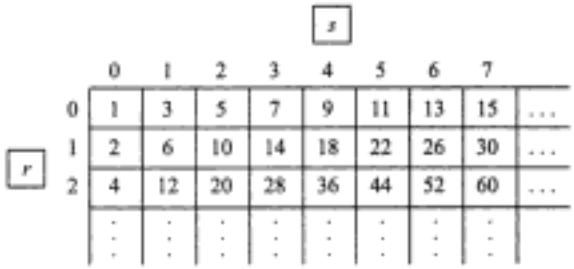


Fig. 14-12

Produtos de Conjuntos e Ordem

14.9 Considere $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$ com a ordem induzida no produto (Seção 14.2) onde $\mathbf{N}$ tem a ordem usual $\leq$. Insira o símbolo correto, $\prec$, $\succ$ ou $\|$ (não-comparável), entre cada um dos seguintes pares de elementos de $\mathbf{N} \times \mathbf{N}$.

(*a*) $(5,7)\_\_(7,1)$ (*c*) $(5,5)\_\_(4,8)$ (*e*) $(7,9)\_\_(4,1)$

(*b*) $(4,6)\_\_(4,2)$ (*d*) $(1,3)\_\_(1,7)$ (*f*) $(7,9)\_\_(8,2)$

Neste caso, $(a, b) \lesssim (a', b')$, desde que $a \leq a'$ e $b \leq b'$. Portanto, $(a, b) \prec (a', b')$ se $a < a'$ e $b \leq b'$ ou $a \leq a'$ e $b < b'$. Logo,

(*a*) $\|$ já que $5 < 7$ mas $7 > 1$. (*c*) $\|$ já que $5 > 4$ and $5 < 8$. (*e*) $\succ$ já que $7 > 4$ e $9 > 1$.

(*b*) $\succ$ já que $4 \geq 4$ e $6 > 2$. (*d*) $\prec$ já que $1 \leq 1$ and $3 < 7$. (*f*) $\|$ já que $7 < 8$ e $9 > 2$.

14.10 Repita o Problema 14.9 usando a ordem lexicográfica de $\mathbf{N}^2 = \mathbf{N} \times \mathbf{N}$.

Aqui $(a, b) \prec (a', b')$ se $a < a'$ ou $a = a'$ mas $b < b'$.

(*a*) $\prec$ já que $5 < 7$. (*c*) $\succ$ já que $5 > 4$. (*e*) $\succ$ já que $7 > 4$.

(*b*) $\succ$ já que $4 = 4$ e $6 > 2$. (*d*) $\prec$ já que $1 = 1$ mas $3 < 7$. (*f*) $\prec$ já que $7 < 8$.

14.11 Considere o alfabeto $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ com a *ordem usual* (*alfabética*) e suponha que o produto $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$ tem a ordem induzida no produto. Insira o símbolo correto, $\prec$, $\succ$ ou $\|$ (não-comparável), entre cada uma das seguintes palavras de duas letras (vistas como elementos de $\mathbf{A} \times \mathbf{A}$):

(*a*) *cx*__*at* (*c*) *cx*__*cz* (*e*) *cx*__*dx*
(*b*) *cx*__*by* (*d*) *cx*__*rs* (*f*) *cx*__*cs*

(*a*) $\succ$ já que $c > a$ e $x > t$. (*c*) $\prec$ já que $c \leq c$ e $x < z$. (*e*) $\prec$ já que $c < d$ e $x \leq x$.
(*b*) $\|$ já que $c > b$ mas $x < y$. (*d*) $\|$ já que $c < r$ mas $x > s$. (*f*) $\succ$ já que $c \geq c$ e $x > s$.

14.12 Repita o Problema 14.11 usando a ordem lexicográfica de $\mathbf{A}^2 = \mathbf{A} \times \mathbf{A}$.

(*a*) $\succ$ já que $c > a$. (*c*) $\prec$ já que $c = c$ e $x < z$. (*e*) $\prec$ já que $c < d$.
(*b*) $\succ$ já que $c > b$. (*d*) $\prec$ já que $c < r$. (*f*) $\succ$ já que $c = c$ e $x > s$.

14.13 Considere o alfabeto $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ com a ordem *usual* (*alfabética*). Suponha que A^*, que consiste em todas as palavras em $\mathbf{A}$, seja ordenado pela ordem comprimento-lexicográfica (semigrupo livre). Ordene os seguintes elementos de A^*:

vela, felino, tu, madeiras, má, túnel, mata, fel, vê, ato

Primeiramente ordene os elementos por comprimento, e depois use a ordem lexicográfica (alfabética):

má, tu, vê, ato, fel, mata, vela, túnel, felino, madeiras

14.14 Repita o Problema 14.13 usando a ordem usual (alfabética) de A^*.

A ordem usual produz:

ato, fel, felino, má, madeiras, mata, tu, túnel, vê, vela

Enumerações Consistentes

14.15 Seja $S = \{a, b, c, d, e\}$ ordenado como na Figura 14-13. Ache todas as possíveis enumerações consistentes $f: S \to \{1, 2, 3, 4, 5\}$.

Como a é o único elemento minimal, $f(a) = 1$, e como e é o único elemento maximal, $f(e) = 5$. Além disso, como b é o único sucessor de a, $f(b) = 2$. As escolhas para c e d são $f(c) = 3$ e $f(d) = 4$ ou vice-versa. Logo, existem duas enumerações possíveis:

(i) $f(a) = 1$, $f(b) = 2$, $f(c) = 3$, $f(d) = 4$, $f(e) = 5$
(ii) $f(a) = 1$, $f(b) = 2$, $f(c) = 4$, $f(d) = 3$, $f(e) = 5$

Enfatizamos que, em geral, não se pode recriar a ordem parcial original a partir de uma enumeração consistente dada.

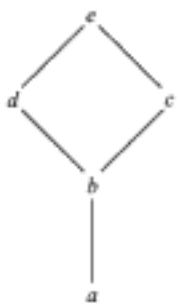


Fig. 14-13

14.16 Prove o Teorema 14.1: suponha que S é um conjunto finito parcialmente ordenado com n elementos. Então, existe uma enumeração consistente $f: S \to \{1, 2, \ldots, n\}$.

A demonstração é por indução sobre o número de elementos n de S. Suponha que $n = 1$, digamos, $S = \{s\}$. Então, $f(s) = 1$ é uma enumeração consistente de S. Agora suponha que $n > 1$ e que o teorema vale para qualquer conjunto parcialmente ordenado com menos do que n elementos. Seja a em S um elemento minimal. (Tal elemento existe, pois S é finito.) Seja $T = S \backslash \{a\}$. Então, T é um conjunto finito parcialmente ordenado com $n-1$ elementos e, portanto, por indução, T admite uma enumeração consistente; digamos $g: T \to \{1, 2, \ldots, n-1\}$. Defina $f: S \to \{1, 2, \ldots, n\}$ por

$$f(x) = \begin{cases} 1, & \text{se } x = a \\ g(x) + 1, & \text{se } x \neq a \end{cases}$$

Então, f é a enumeração consistente requerida.

14.17 Suponha que uma estudante deseja fazer todos os oito cursos de matemática do Problema 14.6, cursando apenas um por semestre.

(*a*) Qual escolha (ou escolhas) ela tem como primeiro e último (oitavo) semestre?

(*b*) Suponha que ela deseje cursar Mat 250 no primeiro ano (primeiro ou segundo semestre) e Mat 240 no último ano (sétimo ou oitavo semestre). Determine todas as maneiras pelas quais ela pode fazer os oito cursos.

(*a*) Pela Figura 14-11, Mat 101 é o único elemento minimal e, portanto, deve ser feito no primeiro semestre; Mat 341 e 500 são os elementos maximais e, logo, um deles deve ser feito no último semestre.

(*b*) Mat 250 não é um elemento minimal e, portanto, deve ser feito no segundo semestre, e Mat 340 não é um elemento maximal, de modo que deve ser feito no sétimo semestre, e Mat 341 no oitavo semestre. Ademais, Mat 500 precisa ser feito no sexto semestre. Apresentamos a seguir as três maneiras possíveis de fazer os oito cursos:

$$[101, 250, 251, 201, 450, 500, 340, 341]$$
$$[101, 250, 201, 251, 450, 500, 340, 341]$$
$$[101, 250, 201, 450, 251, 500, 340, 341]$$

Limites Superior e Inferior, Supremum e Infimum

14.18 Seja $S = \{a, b, c, d, e, f, g\}$ ordenado como na Figura 14-14(*a*), e seja $X = \{c, d, e\}$.

(*a*) Ache os limites inferior e superior de X.

(*b*) Identifique $\sup(X)$, o *supremum* de X, e $\inf(X)$, o *infimum* de X, se existirem.

Os elementos e, f e g sucedem todos os outros elementos de X; portanto, e, f e g são os limites superiores de X. O elemento a precede todo elemento de X; portanto, é o limite inferior de X. Note que b não é um limite inferior, pois b não precede c; de fato, b e c são não-comparáveis.

Como e precede f e g, temos $e = \sup(X)$. Analogamente, como a precede trivialmente todo limite inferior de X, temos $a = \inf(X)$. Note que $\sup(X)$ pertence a X mas $\inf(X)$ não pertence a X.

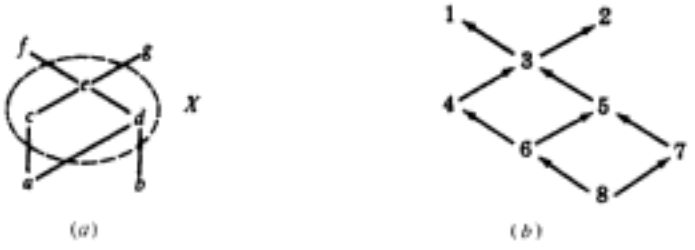


Fig. 14-14

14.19 Seja $S = \{1, 2, 3, \ldots, 8\}$ ordenado como na Figura 14-14(*b*) e seja $A = \{2, 3, 6\}$.

(*a*) Ache os limites superior e inferior de A.

(*b*) Identifique $\sup(A)$ e $\inf(A)$ se existirem.

(*a*) O limite superior é 2, e os limites inferiores são 6 e 8.

(*b*) Neste caso, $\sup(A) = 2$ e $\inf(A) = 6$.

14.20 Repita o Problema 14.19 para o subconjunto $B = \{1, 2, 5\}$.

(*a*) Não existe limite superior para B, pois nenhum elemento sucede ambos, 2 e 5. Os limites inferiores são 6, 7 e 8.

(*b*) Trivialmente, não existe $\sup(A)$, pois não existem limites superiores. Embora A tenha três limites inferiores, não existe $\inf(A)$, já que nenhum limite inferior sucede ambos, 6 e 7.

14.21 Considere o conjunto $\mathbf{Q}$ dos números racionais com a ordem usual $\leq$, e considere o subconjunto D de $\mathbf{Q}$ definido por

$$D = \{x : x \in \mathbf{Q} \text{ e } 8 < x^3 < 15\}$$

(*a*) D é limitado superior ou inferiormente? (*b*) $\sup(D)$ e $\inf(D)$ existem?

(*a*) O subconjunto D é limitado tanto superiormente quanto inferiormente. Por exemplo, 1 é um limite inferior e 100 é um limite superior.

(*b*) $\sup(D)$ não existe. Suponha, por absurdo, que $\sup(D) = x$. Como $\sqrt[3]{15}$ é irracional, $x > \sqrt[3]{15}$. Entretanto, existe um número racional y tal que $\sqrt[3]{15} < y < x$. Logo, y é um limite superior de D também. Isso contradiz a hipótese de que $x = \sup(D)$. Por outro lado, $\inf(D)$ existe. Especificamente, $\inf(D) = 2$.

Conjuntos Isomorfos (Similares), Mapeamentos de Similaridade

14.22 Suponha que um conjunto A parcialmente ordenado é isomorfo a um conjunto B parcialmente ordenado e $f: A \to B$ é um mapeamento de similaridade. As afirmações seguintes são verdadeiras ou falsas?

(*a*) Um elemento $a \in A$ é um primeiro (último, minimal ou maximal) elemento de A se e somente se $f(a)$ é um primeiro (último, minimal ou maximal) elemento de B.

(*b*) Um elemento $a \in A$ precede imediatamente um elemento $a' \in A$, isto é, $a \ll a'$, se e somente se $f(a) \ll f(a')$.

(*c*) Um elemento $a \in A$ tem r sucessores imediatos em A se e somente se $f(a)$ tem r sucessores imediatos em B.

Todas as afirmações são verdadeiras; a estrutura de ordem de A é igual à estrutura de ordem de B.

14.23 Seja S o conjunto ordenado da Figura 14-13. Suponha que $A = \{1, 2, 3, 4, 5\}$ é isomorfo a S e

$$f = \{(a, 1), (b, 3), (c, 5), (d, 2), (e, 4)\}$$

é um mapeamento de similaridade de S em A. Desenhe o diagrama de Hasse de A.

O mapeamento de similaridade f preserva a estrutura de ordem de S e, portanto, f pode visto simplesmente como uma renomeação dos vértices no diagrama de S. Logo, a Figura 14-15 mostra o diagrama de Hasse de A.

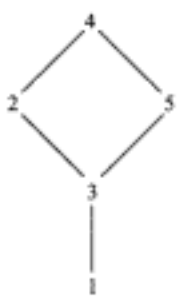


Fig. 14-15

14.24 Seja $A = \{1, 2, 3, 4, 5\}$ ordenado como na Figura 14-15. Ache o número n de mapeamentos de similaridade $f: A \to A$.

Como 1 é o único elemento minimal de A e 4 é o único elemento maximal, devemos ter $f(1) = 1$ e $f(4) = 4$. Ademais, $f(3) = 3$, pois 3 é o único sucessor imediato de 1. Por outro lado, existem duas possibilidades para $f(2)$ e $f(5)$, isto é, $f(2) = 2$ e $f(5) = 5$, ou $f(2) = 5$ e $f(5) = 2$. Conseqüentemente, $n = 2$.

14.25 Dê um exemplo de um conjunto finito $X = (A, R)$ que não é linearmente ordenado isomorfo a $Y = (A, R^{-1})$, o conjunto A com a ordem inversa.

Seja R a ordenação parcial de $A = \{a, b, c, d, e\}$ representada na Figura 14-16(a). Então, a Figura 14-16(b) mostra A com a ordem inversa R^{-1}. (O diagrama de A é simplesmente virado de cabeça para baixo para obter R^{-1}.) Note que os dois diagramas são idênticos, exceto pelos rótulos.

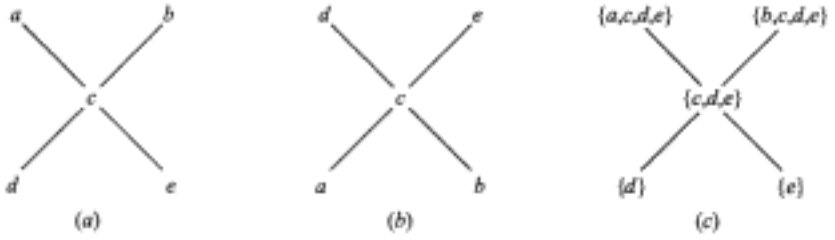


Fig. 14-16

14.26 Seja A um conjunto ordenado e, para cada $a \in A$, denote por $p(a)$ o conjunto dos predecessores de a:

$$p(a) = \{x : x \precsim a\}$$

(denominado o *conjunto predecessor* de a.) Seja $p(A)$ a coleção de todos os conjuntos predecessores de elementos de A, ordenado pela operação de inclusão.

(a) Mostre que A e $p(A)$ são isomorfos provando que o mapeamento $f: A \to p(A)$, definido por $f(a) = p(a)$, é um mapeamento de similaridade de A sobre $p(A)$.

(b) Ache o diagrama de Hasse de $p(A)$ para o conjunto A da Figura 14-16(a).

(a) Primeiramente mostre que f preserva a relação de ordem de A. Suponha que $a \precsim b$. Seja $x \in p(a)$. Então, $x \precsim a$, e $x \precsim b$; logo, $x \in p(b)$. Logo, $p(a) \subseteq p(b)$. Suponha que $a \parallel b$ (não-comparável). Então, $a \in p(a)$ mas $a \notin p(b)$; portanto, $p(a) \not\subseteq p(b)$. Similarmente, $b \in p(b)$ mas $b \notin p(a)$; logo, $p(b) \not\subseteq p(a)$. Portanto, $p(a) \parallel p(b)$. Logo, f preserva ordem.

Agora, resta mostrar que f é injetora e sobrejetora. Suponha que $y \in p(a)$. Então, $y = p(a)$ para algum $a \in A$. Logo, $f(a) = p(a) = y$ e, logo, f é sobrejetora sobre $p(A)$. Suponha que $a \neq b$. Então, $a \prec b$, $b \prec a$ ou $a \parallel b$. No primeiro e no terceiro casos, $b \in p(b)$ mas $b \notin p(a)$ e, no segundo caso, $a \in p(a)$ mas $a \notin p(b)$. Conseqüentemente, nos três casos, temos $p(a) \neq p(b)$. Portanto, f é injetora.

Conseqüentemente, f é um mapeamento de similaridade de A sobre $p(A)$ e assim, $A \simeq p(A)$.

(b) Os elementos de $p(A)$ são:

$$p(a) = \{a, c, d, e\}, \qquad p(b) = \{b, c, d, e\}, \qquad p(c) = \{c, d, e\}, \qquad p(d) = \{d\}, \qquad p(e) = \{e\}$$

A Figura 14-16(c) mostra o diagrama de $p(A)$ ordenado pela inclusão de conjuntos. Observe que os diagramas nas Figuras 14-16(a) e (c) são idênticos, exceto pelos rótulos dos vértices.

Conjuntos Bem-Ordenados

14.27 Mostre o princípio da indução transfinita: seja A um subconjunto de um conjunto bem-ordenado S com as duas propriedades seguintes: (i) $a_0 \in A$. (ii) Se $s(a) \subseteq A$, então $a \in S$. Então, $A = S$.

(Aqui a_0 é o primeiro elemento de a e $s(a)$ é o segmento inicial de a, i.e., o conjunto de todos os elementos que precedem a estritamente.) Suponha que $A \neq S$. Seja $B = S \backslash A$. Então, $B \neq \emptyset$. Como S é bem-ordenado, B tem um primeiro elemento b_0. Cada elemento $x \in s(b_0)$ precede b_0 e, portanto, não pertence a B. Logo, todo $x \in s(b_0)$ pertence a A; portanto, $s(b_0) \subseteq A$. Por (ii), $b_0 \in A$. Isso contradiz a hipótese de que $b_0 \in S \backslash A$. Logo, a hipótese inicial de que $A \neq S$ não é verdade; em outras palavras, $A = S$.

14.28 Seja S um conjunto bem-ordenado com um primeiro elemento a_0. Defina um *elemento limite* de S.

Um elemento $b \in S$ é um elemento limite se $b \neq a_0$ e b não tem predecessor imediato.

14.29 Seja $S = (\mathbf{N}, \precsim)$ ordenado como no Problema 14.8. (Veja a Figura 14-12.) S tem elementos limite?

Como indicado pela Figura 14-12, toda potência de 2, isto é, 1, 2, 4, 8,..., não tem predecessor imediato, e, portanto, é um elemento limite de S.

14.30 Seja S um conjunto bem-ordenado. Seja $f: S \to S$ um mapeamento de similaridade de S em S. Prove que, para todo $a \in S$, $a \precsim f(a)$.

Seja $D = \{x: f(x) \prec x\}$. Se D for vazio, então a afirmação é verdadeira. Suponha que $D \neq \varnothing$. Como D é bem-ordenado, D tem um primeiro elemento, digamos, d_0. Como $d_0 \in D$, temos $f(d_0) \prec d_0$. Como f é um mapeamento de similaridade,

$$f(d_0) \prec d_0 \qquad \text{implica} \qquad f(f(d_0)) \prec f(d_0)$$

Logo, $f(d_0)$ também pertence a D. Mas $f(d_0) \prec d_0$ e $f(d_0) \in D$ contradizem o fato de que d_0 é o primeiro elemento de D. Portanto, a hipótese inicial de que $D \neq \varnothing$ leva a uma contradição. Conseqüentemente, D é vazio e a afirmação é verdadeira.

14.31 Seja A um conjunto bem-ordenado. Seja $s(A)$ a coleção de todos os segmentos iniciais $s(a)$ dos elementos $a \in A$ ordenados pela inclusão de conjuntos. Prove que A é isomorfo a $s(A)$ mostrando que o mapeamento $f: A \to s(A)$, definido por $f(a) = s(a)$, é um mapeamento de similaridade de A sobre $s(A)$. (Compare com o Problema 14-26.)

Mostramos primeiramente que f é um mapeamento injetor e sobrejetor. Suponha que $y \in s(A)$. Então, $y = s(a)$ para algum $a \in A$. Logo, $f(a) = s(a) = y$ e assim f é sobrejetora. Suponha que $x \neq y$. Então, um precede o outro, digamos, $x \prec y$. Então, $x \in s(y)$. Mas $x \notin s(x)$. Logo, $s(x) \neq s(y)$. Por isso, f é também injetora.

Resta apenas mostrar que f preserva ordem, isto é,

$$x \precsim y \qquad \text{se e somente se} \qquad s(x) \subseteq s(y)$$

Suponha que $x \precsim y$. Se $a \in s(x)$, então $a \prec x$ e, portanto, $a \prec y$; logo, $a \in s(y)$. Então, $s(x) \subseteq s(y)$. Por outro lado, suponha que $x \not\precsim y$, isto é, $x \succ y$. Então, $y \in s(x)$. Mas $y \notin s(y)$; portanto, $s(x) \not\subseteq s(y)$. Em outras palavras, $x \precsim y$ se e somente se $s(x) \subseteq s(y)$.

Conseqüentemente, f é um mapeamento de similaridade de A sobre $S(A)$, e portanto, $A \simeq s(A)$.

Reticulados

14.32 Escreva o dual de cada uma das declarações.

(*a*) $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$; (*b*) $(a \wedge b) \vee a = a \wedge (b \vee a)$.

Troque $\vee$ por $\wedge$ e $\wedge$ por $\vee$ em cada uma das declarações para obter a declaração dual.

(*a*) $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$.

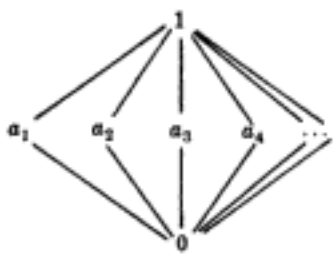
(*b*) $(a \vee b) \wedge a = a \vee (b \wedge a)$.

14.33 Dê o exemplo de um reticulado infinito L de comprimento finito.

Seja $L = \{0, 1, a_1, a_2, a_3, \ldots\}$ e seja L ordenado como na Figura 14-17; isto é, para cada $n \in \mathbf{N}$, temos

$$0 < a_n < 1$$

Então, L tem comprimento finito, pois L não tem subconjunto infinito linearmente ordenado.



Fig, 14-17

14.34 Prove o Teorema 14.4: seja L um reticulado. Então, (i) $a \wedge b = a$ se e somente se $a \vee b = b$. (ii) A relação $a \precsim b$ (definida por $a \wedge b = a$ ou $a \vee b = b$) é uma ordem parcial em L.

(i) Suponha que $a \wedge b = a$. Usando a lei da absorção no primeiro passo, temos

$$b = b \vee (b \wedge a) = b \vee (a \wedge b) = b \vee a = a \vee b$$

Agora suponha que $a \vee b = b$. Usando novamente a lei da absorção no primeiro passo, temos

$$a = a \wedge (a \vee b) = a \wedge b$$

Então, $a \wedge b = a$ se e somente se $a \vee b = b$.

(ii) Para todo $a \in L$, temos $a \wedge a = a$ pela idempotência. Portanto, $a \precsim a$ e, logo, $\precsim$ é reflexiva.

Suponha que $a \precsim b$ e $b \precsim a$. Então, $a \wedge b = a$ e $b \wedge a = b$. Portanto, $a = a \wedge b = b \wedge a$ e, logo, $\precsim$ é anti-simétrica.

Finalmente, suponha que $a \precsim b$ e $b \precsim c$. Então, $a \wedge b = a$ e $b \wedge c = b$. Logo,

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$$

Portanto, $a \precsim c$, e assim, $\precsim$ é transitiva. Conseqüentemente, $\precsim$ é uma ordem parcial em L.

14.35 Quais dos conjuntos parcialmente ordenados da Figura 14-18 são reticulados?

Um conjunto parcialmente ordenado é um reticulado se e somente se $\sup(x, y)$ e $\inf(x, y)$ existem para todo par x, y no conjunto. Apenas (c) não é um reticulado, já que $\{a, b\}$ tem três limites superiores, c, d e I, e nenhum deles precede os outros dois, i.e., não existe $\sup(a, b)$.

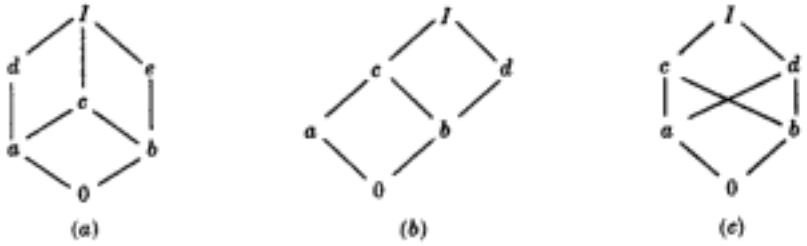


Fig. 14-18

14.36 Considere o reticulado da Figura 14-18(a).

(a) Quais elementos não nulos são irredutíveis por disjunção?

(b) Quais elementos são átomos?

(c) Quais dos seguintes são sub-reticulados de L?

$$L_1 = \{0, a, b, I\}, \qquad L_2 = \{0, a, e, I\}$$
$$L_3 = \{a, c, d, I\}, \qquad L_4 = \{0, c, d, I\}$$

(d) L é distributivo?

(e) Ache, se existirem, complementos para os elementos a, b e c.

(f) L é um reticulado complementado?

(a) Os elementos não nulos com um único predecessor imediato são irredutíveis por disjunção. Portanto, a, b, d e e são irredutíveis por disjunção.

(b) Os elementos que sucedem 0 imediatamente são átomos; portanto, a e b são átomos.

(c) Um subconjunto L' é um reticulado se é fechado sob $\wedge$ e $\vee$. L_1 não é um reticulado, já que $a \vee b = c$, que não pertence a L_1. O conjunto L_4 não é um sub-reticulado pois $c \wedge d = a$ não pertence a L_4. L_2 e L_3 são sub-reticulados.

(d) L não é distributivo já que $M = \{0, a, d, e, I\}$ é um sub-reticulado isomorfo ao reticulado não distributivo da Figura 14-7(a).

(e) Temos $a \wedge e = 0$ e $a \vee e = I$; logo, a e e são complementos. b e d também são complementos. Entretanto, c não tem complemento.

(f) L não é um reticulado complementado, pois c não tem complemento.

14.37 Considere o reticulado M da Figura 14-18(b).

(a) Ache os elementos irredutíveis por disjunção e os átomos de M.

(b) M é distributivo?

(c) M é complementado?

(a) Os elementos não nulos com predecessor único são a, b e d, e dentre estes três, apenas a e b são átomos, pois seu único predecessor é 0.

(b) M é distributivo, pois não possui sub-reticulado isomorfo a algum dos reticulados da Figura 14-7.

(c) M não é complementado, já que b não tem complemento. Note que a é a única solução para $b \wedge x = 0$, mas $b \vee a = c \neq I$.

14.38 Prove o Teorema 14.8: seja L um reticulado finito distributivo. Então, todo a em L pode ser escrito de maneira única (exceto pela ordem) como uma disjunção de elementos irredutíveis por disjunção.

Como L é finito, podemos escrever a como uma disjunção de elementos irredutíveis por disjunção como discutimos na Seção 14-9. Assim, precisamos provar apenas a unicidade. Suponha que

$$a = b_1 \vee b_2 \vee \cdots \vee b_r = c_1 \vee c_2 \vee \cdots \vee c_s$$

onde os bs são não redundantes e irredutíveis por disjunção e os cs são não redundantes e irredutíveis. Para todo i dado, temos

$$b_i \precsim (b_1 \vee b_2 \vee \cdots \vee b_r) = (c_1 \vee c_2 \vee \cdots \vee c_s)$$

Portanto,

$$b_i = b_i \wedge (c_1 \vee c_2 \vee \cdots \vee c_s) = (b_i \wedge c_1) \vee (b_i \wedge c_2) \vee \cdots \vee (b_i \wedge c_s)$$

Como b_i é irredutível por disjunção, existe um j tal que $b_i = b_i \wedge c_j$, e assim, $b_i \precsim c_j$. Por um argumento análogo, para c_j existe um b_k tal que $c_j \precsim b_k$. Portanto,

$$b_i \precsim c_j \precsim b_k$$

o que dá $b_i = c_j = b_k$, já que os b são não redundantes. Logo, a representação de a é única, exceto pela ordem.

14.39 Prove o Teorema 14.10: seja L um reticulado complementado com complementos únicos. Então, os elementos de L irredutíveis por disjunção diferentes de 0 são seus átomos.

Suponha que a é irredutível por disjunção e não é um átomo. Então, a tem um único predecessor imediato $b \neq 0$. Seja b' o complemento de b. Como $b \neq 0$, temos $b' \neq I$. Se a precede b', então $b \precsim a \precsim b'$ e, logo, $b \wedge b' = b'$, o que é impossível, já que $b \wedge b' = I$. Logo, a não precede b', e, portanto, $a \wedge b'$ deve preceder a estritamente. Como b é o único predecessor imediato de a, também temos que $a \wedge b'$ precede b como na Figura 14-19. Mas a e b' precede b'. Portanto,

$$a \wedge b' \precsim \inf(b, b') = b \wedge b' = 0$$

Logo, $a \wedge b' = 0$. Como $a \vee b = a$, também temos que

$$a \vee b' = (a \vee b) \vee b' = a \vee (b \vee b') = a \vee I = I$$

Portanto, b' é um complemento de a. Como os complementos são únicos, $a = b$. Isso contradiz a hipótese de que b é um predecessor imediato de a. Portanto, os únicos elementos irredutíveis por disjunção de L são os seus átomos.

Fig. 14-19

Problemas Complementares

Conjuntos Ordenados e Subconjuntos

14.40 Seja $A = \{1, 2, 3, 4, 5, 6\}$ ordenado como na Figura 14-20(a).

(a) Ache todos os elementos minimais e maximais de A.

(b) A tem um primeiro ou último elemento?

(c) Ache todos os subconjuntos linearmente ordenados de A, cada um dos quais contendo pelo menos três elementos.

(a) (b) (c)

Fig. 14-20

14.41 Seja $B = \{a, b, c, d, e, f\}$ ordenado como na Figura 14-20(b).

(a) Ache todos os elementos minimais e maximais de B.

(b) B tem um primeiro ou último elemento?

(c) Ache o número de enumerações consistentes de B em relação ao conjunto $\{1, 2, 3, 4, 5, 6\}$ e cite duas.

14.42 Seja $C = \{1, 2, 3, 4\}$ ordenado como na Figura 14-20(c). Denote por $L(C)$ a coleção de todos os subconjuntos não vazios linearmente ordenados pela relação de inclusão. Desenhe o diagrama de $L(C)$.

14.43 Desenhe os diagramas das partições de m (veja o Exemplo 14.14) onde (a) $m = 4$; (b) $m = 6$.

14.44 Denote por $\mathbf{D}_m$ os divisores positivos de m ordenados por divisibilidade. Desenhe os diagramas de Hasse de:

(a) $\mathbf{D}_{12}$; (b) $\mathbf{D}_{15}$; (c) $\mathbf{D}_{16}$; (d) $\mathbf{D}_{17}$.

14.45 Seja $S = \{a, b, c, d, e, f\}$ um conjunto parcialmente ordenado. Suponha que existam exatamente seis pares de elementos tais que o primeiro precede imediatamente o segundo como a seguir:

$$f \ll a, \quad f \ll d, \quad e \ll b, \quad c \ll f, \quad e \ll c, \quad b \ll f$$

(a) Ache todos os elementos minimais e maximais de S.

(b) S tem um primeiro ou último elemento?

(c) Ache todos os pares de elementos, se existirem, que sejam não-comparáveis.

14.46 Decida se cada uma das afirmações seguintes é verdadeira ou falsa e, se falsa, dê um contra-exemplo:

(a) Se um conjunto parcialmente ordenado S tem apenas um elemento maximal a, então a é um último elemento.

(b) Se um conjunto finito parcialmente ordenado S tem apenas um elemento maximal a, então a é um último elemento.

(b) Se um conjunto s linearmente ordenado tem apenas um elemento maximal a, então a é um último elemento.

14.47 Seja $S = \{a, b, c, d, e\}$ ordenado como na Figura 14-21(a).

(a) Ache todos os elementos maximais e minimais de S.

(b) S tem algum primeiro ou último elemento?

(c) Ache todos os subconjuntos de S nos quais c é um elemento minimal.

(d) Ache todos os subconjuntos de S nos quais c é um primeiro elemento.

(e) Liste todos os subconjuntos linearmente ordenados com três ou mais elementos.

Fig. 14-21

14.48 Seja $S = \{a, b, c, d, e, f\}$ ordenado como na Figura 14-21(*b*)

(*a*) Ache todos os elementos maximais e minimais de S.

(*b*) S tem algum primeiro ou último elemento?

(*c*) Liste todos os subconjuntos linearmente ordenados com três ou mais elementos.

14.49 Seja $S = \{a, b, c, d, e, f, g\}$ ordenado como na Figura 14-14(*a*). Ache o número n de subconjuntos linearmente ordenados de S com: (*a*) quatro elementos; (*b*) cinco elementos.

14.50 Seja $S = \{1, 2, \ldots, 7, 8\}$ ordenado como na Figura 14-21(*b*). Ache o número n de subconjuntos linearmente ordenados de S com: (*a*) cinco elementos; (*b*) seis elementos.

Enumerações Consistentes

14.51 Seja $S = \{a, b, c, d, e\}$ ordenado como na Figura 14-21(*a*). Liste todas as enumerações consistentes de S em $\{1, 2, 3, 4, 5\}$.

14.52 Seja $S = \{a, b, c, d, e, f\}$ ordenado como na Figura 14-21(*b*). Ache o número n de enumerações consistentes de S em $\{1, 2, 3, 4, 5, 6\}$.

14.53 Suponha que as enumerações a seguir são enumerações consistentes de um conjunto ordenado $A = \{a, b, c, d\}$:

$$[(a,1),(b,2),(c,3),(d,4)], \qquad [(a,1),(b,3),(c,2),(d,4)], \qquad [(a,1),(b,4),(c,2),(d,3)]$$

Supondo que o diagrama de Hasse D de S é conexo, desenhe D.

Ordem e Conjuntos, Produto e Fechos de Kleene

14.54 Seja $M = \{2, 3, 4, \ldots\}$ e seja $M^2 = M \times M$ ordenado como a seguir:

$$(a,b) \precsim (c,d) \qquad \text{se } a \mid c \text{ e } b \leq d$$

Ache todos os elementos minimais e maximais de $M \times M$.

14.55 Considere o alfabeto $A = \{a, b, c, \ldots, y, z\}$ com a ordem usual (alfabética). Lembre que o fecho de Kleene A^* consiste em todas as palavras em A. Seja L o conjunto contendo os elementos seguintes em A^*:

gelo, ou, ano, ge, ai, ábaco, galo, ode, ar, ocaso

(*a*) Ordene L na ordem comprimento-lexicográfica, i.e., primeiramente por comprimento e depois alfabeticamente.

(*b*) Ordene R pela ordem alfabética.

14.56 Considere os conjuntos ordenados A e B que aparecem na Figura 14-20(*a*) e (*b*), respectivamente. Suponha que $S = A \times B$ tem a ordem induzida no produto, i.e.,

$$(a,b) \precsim (a',b') \qquad \text{se } a \precsim a' \text{ e } b \precsim b'$$

Insira o símbolo correto $\prec$, $\succ$ ou $\|$ entre cada par de elementos de S:

(*a*) $(4,b)$ ____ $(2,e)$ (*b*) $(3,a)$ ____ $(6,f)$

(*c*) $(5,d)$ ____ $(1,a)$ (*d*) $(6,e)$ ____ $(2,b)$

14.57 Considere $\mathbf{N} = \{1, 2, 3, \ldots\}$ e $\mathbf{A} = \{a, b, c, \ldots, y, z\}$ com a ordem usual e $S = \mathbf{N} \times \mathbf{A}$ ordenado lexicograficamente. Ordene os seguintes elementos de S.

$$(2, z), \quad (1, c), \quad (2, c), \quad (1, y), \quad (4, b), \quad (4, z), \quad (3, b) \quad (2, a)$$

Limites Superior e Inferior, Supremum e Infimum

14.58 Seja $S = \{a, b, c, d, f, g\}$ ordenado como na Figura 14-14(*a*). Considere o subconjunto $A = \{a, c, d\}$ de S.

(*a*) Ache o conjunto dos limites superiores de A.

(*b*) Ache o conjunto dos limites inferiores de A.

(*c*) Existe sup(A)?

(*d*) Existe inf(A)?

14.59 Repita o Problema 14.58 para o subconjunto $B = \{b, c, e\}$ de S.

14.60 Seja $S = \{1, 2, \ldots, 7, 8\}$ ordenado como na Figura 14-14(*b*). Considere o subconjunto $A = \{3, 6, 7\}$ de S.

(*a*) Ache o conjunto dos limites superiores de A.

(*b*) Ache o conjunto dos limites inferiores de A.

(*c*) Existe sup(A)?

(*d*) Existe inf(A)?

14.61 Repita o Problema 14.60 para o subconjunto $B = \{1, 2, 4, 7\}$ de S.

14.62 Considere o conjunto dos números racionais $\mathbf{Q}$ com a ordem usual $\leq$. Seja $A = \{x : x \in \mathbf{Q} \text{ e } 5 < x^3 < 27\}$.

(*a*) A é limitado superior ou inferiormente?

(*b*) Existe sup(A) ou inf(A)?

14.63 Considere o conjunto dos números reais $\mathbf{R}$ com a ordem usual $\leq$. Seja $A = \{x : x \in \mathbf{Q} \text{ e } 5 < x^3 < 27\}$.

(*a*) A é limitado superior ou inferiormente?

(*b*) Existe sup(A) ou inf(A)?

Conjuntos Isomorfos (Similares), Mapeamentos de Similaridades

14.64 Seja S o conjunto ordenado da Figura 14-21(*a*). Suponha que $A = \{1, 2, 3, 4, 5\}$ é isomorfo a S e que o mapeamento descrito a seguir é um mapeamento de similaridade de S em A.

$$f = \{(a, 1), \ (b, 4), \ (c, 5), \ (d, 2), \ (e, 3)\}$$

Desenhe o diagrama de Hasse de A.

14.65 Ache o número de conjuntos parcialmente ordenados não isomorfos com três elementos, a, b e c, e desenhe seus diagramas de Hasse.

14.66 Ache o número de conjuntos conexos parcialmente ordenados não isomorfos com quatro elementos, a, b, c e d, e desenhe seus diagramas de Hasse.

14.67 Ache o número de mapeamentos de similaridade $f: S \to S$ se S é o conjunto ordenado em: (*a*) Figura 14-20(*a*); (*b*) Figura 14-20(*b*); (*c*) Figura 14-20(*c*).

14.68 Mostre que a relação de isomorfismo $A \simeq B$ para conjuntos ordenados é uma relação de equivalência, isto é: (*a*) $A \simeq A$ para qualquer conjunto ordenado A. (*b*) Se $A \simeq B$ e $B \simeq C$, então $A \simeq C$.

Conjuntos Bem-Ordenados

14.69 Suponha que a união S de conjuntos $A = \{a_1, a_2, a_3, \ldots\}$, $B = \{b_1, b_2, b_3, \ldots\}$, $C = \{c_1, c_2, c_3, \ldots\}$ seja ordenada como descrito a seguir:

$$S = \{A; \ B; \ C\} = \{a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots\}$$

(*a*) Mostre que S é bem-ordenado.

(*b*) Ache todos os elementos limite de S.

(*c*) Mostre que S não é isomorfo a $\mathbf{N}$ com a ordem usual $\leq$.

14.70 Seja $A = \{a, b, c\}$ ordenado linearmente por $a < b < c$, e seja $\mathbf{N} = \{1, 2, \ldots\}$ com a ordem usual $\leq$.

(*a*) Mostre que $S = \{A; \mathbf{N}\}$ é isomorfo a $\mathbf{N}$.

(*b*) Mostre que $S' = \{\mathbf{N}; A\}$ não é isomorfo a $\mathbf{N}$.

14.71 Suponha que A é um conjunto bem-ordenado sob a relação de $\precsim$, e suponha que A também é bem-ordenado pela relação inversa $\succsim$. Descreva A.

14.72 Suponha que A e B são conjuntos isomorfos bem-ordenados. Mostre que existe apenas um mapeamento de similaridade $f: A \to B$.

14.73 Seja S um conjunto bem-ordenado. Para todo $a \in S$, o conjunto $s(a) = \{x: x \prec a\}$ é denominado um segmento inicial de a. Mostre que S não pode ser isomorfo a nenhum dos seus segmentos iniciais. (*Sugestão:* use o Problema 14.30.)

14.74 Suponha que $s(a)$ e $s(b)$ são segmentos iniciais distintos de um conjunto bem-ordenado S. Mostre que $s(a)$ e $s(b)$ não podem ser isomorfos. (*Sugestão:* use o Problema 14.73.)

Reticulados

14.75 Considere o reticulado L da Figura 14-22(*a*). (*a*) Ache todos os sub-reticulados com cinco elementos. (*b*) Ache todos os elementos irredutíveis por disjunção e átomos. (*c*) Ache os complementos de a e b, se existirem. (*d*) L é distributivo? Complementado?

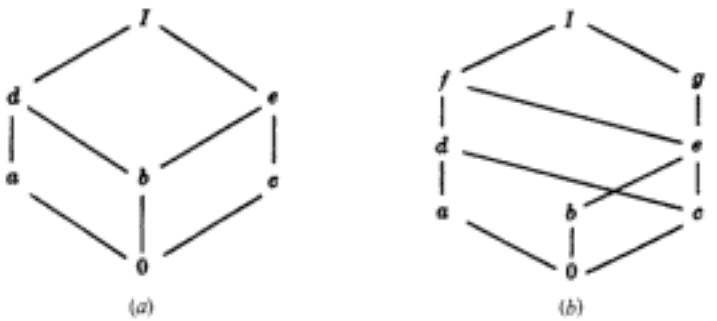


Fig. 14-22

14.76 Considere o reticulado M na Figura 14-22(*b*). (*a*) Ache todos os elementos irredutíveis por disjunção. (*b*) Ache os átomos. (*c*) Ache os complementos de a e b, se existirem. (*d*) Expresse cada x em M como a disjunção de elementos não-redundantes irredutíveis por disjunção. (*e*) M é distributivo? Complementado?

14.77 Considere o reticulado limitado L da Figura 14-23(*a*).

(*a*) Ache os complementos (se existirem) de e e f.

(*b*) Expresse I como uma decomposição de disjunções irredutíveis não redundantes de tantas maneiras quanto possível.

(*c*) L é distributivo?

(*d*) Descreva o isomorfismo de L com o próprio L.

14.78 Considere o reticulado limitado L da Figura 14-23(*b*)

(*a*) Ache os complementos (se existirem) de a e f.

(*b*) Expresse I como uma decomposição de disjunções irredutíveis não redundantes de tantas maneiras quanto possível.

(*c*) L é distributivo?

(*d*) Descreva o isomorfismo de L com o próprio L.

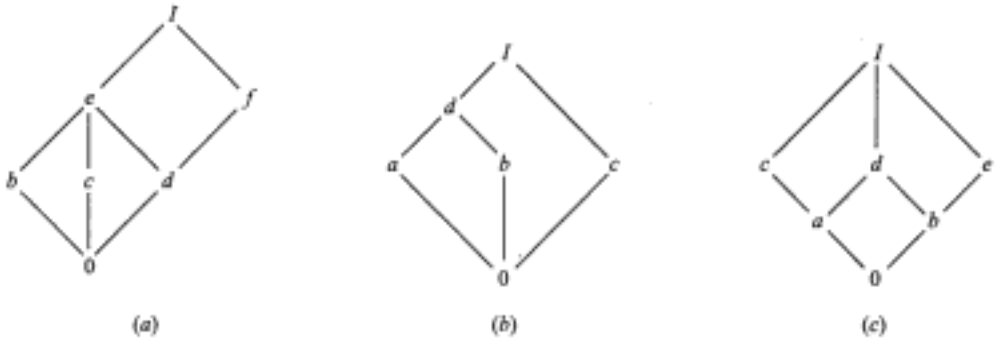
14.79 Considere o reticulado limitado L na Figura 14-23(c)

(a) Ache os complementos (se existirem) de a e c.

(b) Expresse I como uma decomposição de disjunções irredutíveis não redundantes de tantas maneiras quanto possível.

(c) L é distributivo?

(d) Descreva o isomorfismo de L com o próprio L.



(a) (b) (c)

Fig. 14-23

14.80 Considere o reticulado $\mathbf{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ dos divisores de 60 ordenados por divisibilidade. (a) Desenhe o diagrama de $\mathbf{D}_{60}$. (b) Quais os elementos irredutíveis por disjunção? E os átomos? (c) Ache os complementos de 2 e 10, se existirem. (d) Expresse cada número x como a disjunção de um número mínimo de elementos não redundantes irredutíveis por disjunção.

14.81 Considere o reticulado $\mathbf{N}$ de inteiros positivos ordenados por divisibilidade. (a) Quais elementos são irredutíveis por disjunção? (b) Quais elementos são átomos?

14.82 Mostre que as seguintes formas "fracas" das leis de distributividade valem para qualquer reticulado.

(a) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(b) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

14.83 Seja $S = \{1, 2, 3, 4\}$. Usando a notação $[12, 3, 4] \equiv [\{1, 2\}, \{3\}, \{4\}]$, três partições de S são:

$$P_1 = [12, 3, 4], \qquad P_2 = [12, 34], \qquad P_3 = [13, 2, 4]$$

(a) Ache as outras nove partições de S.

(b) Seja L a coleção de 12 partições de S ordenadas por *refinamento*, i.e., $P_i \precsim P_j$ se cada célula de P_i for um subconjunto de uma célula de P_j. Por exemplo, $P_1 \precsim P_2$, mas P_2 e P_3 são não comparáveis. Mostre que L é um reticulado limitado e desenhe seu diagrama.

14.84 Um elemento a em um reticulado L é dito irredutível por conjunção se $a = x \wedge y$ implicar $a = x$ ou $a = y$. Ache todos os elementos irredutíveis por conjunção em: (a) Figura 13-22(a); (b) Figura 13-22(b); (c) $\mathbf{D}_{60}$ (veja o Problema 14.80).

14.85 Um reticulado M é dito *modular* se toda vez que $a \leq c$ vale a lei

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

(a) Prove que todo reticulado distributivo é modular.

(b) Verifique que o reticulado não distributivo da Figura 14-7(b) é modular; portanto, o converso de (a) não é verdade.

(c) Prove que o reticulado não distributivo da Figura 14-7(a) não é modular. [De fato, pode-se provar que todo reticulado não modular contém um sub-reticulado isomorfo à Figura 14-7(a).]

Hidden page

14.45 *Sugestão*: desenhe o diagrama de S. (*a*) Minimal, e; maximal, a,d. (*b*) Primeiro, e; último, nenhum. (*c*) $\{a, d\}$, $\{b, c\}$.

14.46 (*a*) Falso. Exemplo: $\mathbf{N} \cup \{a\}$ onde $1 \ll a$, e $\mathbf{N}$ ordenado por $\leq$. (*b*) Verdadeiro. (*c*) Verdadeiro.

14.47 (*a*) Minimal, a; maximal, d e e. (*b*) Primeiro, a; último, nenhum. (*c*) Qualquer subconjunto que contém c e omite a; isto é: c, cb, cd, ce, cbd, cbe, cde, $cbde$. (*d*) c, cd, ce, cde. (*e*) abd, acd, ace.

14.48 (*a*) Minimal, a e b; maximal, e e f. (*b*) Primeiro, nenhum; último, nenhum. (*c*) ace, $acef$, bce, bcf, bdf.

14.49 (*a*) Quatro. (*b*) Nenhum.

14.50 (*a*) Seis. (*b*) Nenhum.

14.51 $abcde$, $abced$, $acbde$, $acbed$, $acebd$.

14.52 11.

14.53 $a \ll b$, $a \ll c$, $c \ll d$.

14.54 Minimal, $(p, 2)$ onde p é um primo. Maximal, nenhum.

14.55 (*a*) ai, ar, ge, ou, ano, ode, galo, gelo, ábaco, ocaso.

(*b*) ábaco, ai, ano, ar, galo, ge, gelo, ocaso, ode, ou.

14.56 (*a*) $\|$; (*b*) $>$; (*c*) $\|$; (*d*) $<$.

14.57 $1c$, $1y$, $2a$, $2c$, $2z$, $3b$, $4b$, $4z$.

14.58 (*a*) e, f, g; (*b*) a; (*c*) $\sup(A) = e$; (*d*) $\inf(A) = a$.

14.59 (*a*) e, f, g; (*b*) nenhum; (*c*) $\sup(B) = e$; (*d*) nenhum.

14.60 (*a*) 1, 2, 3; (*b*) 8; (*c*) $\sup(A) = 3$; (*d*) $\inf(A) = 8$.

14.61 (*a*) Nenhum; (*b*) 8; (*c*) nenhum; (*d*) $\inf(B) = 8$.

14.62 (*a*) Ambos; (*b*) $\sup(A) = 3$; $\inf(A)$ não existe.

14.63 (*a*) Ambos; (*b*) $\sup(A) = 3$; $\inf(A) = \sqrt[3]{5}$.

14.64 Veja a Figura 14-27.

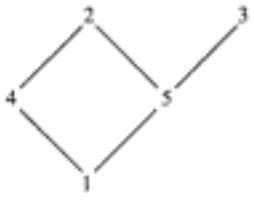


Fig. 14-27

14.65 Quatro: (1) a, b, c; (2) $a, b \ll c$; (3) $a \ll b, a \ll c$; (4) $a \ll b \ll c$.

14.66 Veja a Figura 14-28.

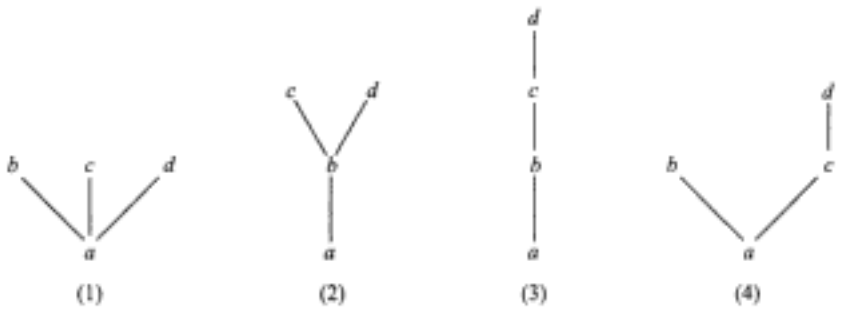


Fig. 14-28

14.67 (*a*) Um: mapeamento identidade; (*b*) um; (*c*) dois.

14.69 (*b*) b_1, c_1. (*c*) **N** não tem pontos limite.

14.70 (*a*) Defina f: $S \to \mathbf{N}$ por $f(a) = 1, f(b) = 2, f(3) = 3, f(n) = n + 3$.

(*b*) O elemento a é um ponto limite de S', mas **N** não tem pontos limite.

14.71 A é um conjunto finito linearmente ordenado.

14.75 (*a*) Seis: $0abd1$, $0acd1$, $0ade1$, $0bce1$, $0ace1$, $0cde1$.

(*b*) (i) $a, b, e, 0$; (*b*) (ii) a, b, c.

(*c*) c e e são complementos de a. b não tem complementos.

(*d*) Não. Não.

14.76 (*a*) $a, b, c, g, 0$. (*b*) a, b, c. (*c*) a: g; b: nenhum.

(*d*) $1 = a \vee g, f = a \vee b = a \vee c, e = b \vee c, d = a \vee c$. Outros elementos são irredutíveis por disjunção.

(*e*) Não. Não.

14.77 (*a*) e não tem nenhum; f tem b e c.

(*b*) $1 = c \vee d \vee f = b \vee c \vee f = b \vee d \vee f$.

(*c*) Não, pois decomposições não são únicas.

(*d*) Dois: $0, d, e, f, 1$ devem ser mapeados em si mesmo. Portanto, $F = 1_L$, o mapeamento identidade em L, ou $F = \{(b, c), (c, b)\}$.

14.78 (*a*) a tem c, c tem a e b. (*b*) $1 = a \vee c = b \vee c$.

(*c*) Não. (*d*) Dois: $0, c, d, 1$ devem ser mapeados em si mesmo. Portanto, $f = 1_L$, ou $F = \{(a, b), (b, a)\}$.

14.79 (*a*) a tem e, c tem b e e. (*b*) $1 = a \vee e = b \vee c = c \vee e$.

(*c*) Não. (*d*) Dois: $0, d, 1$ são mapeados em si mesmo. Então, $f = 1_L$ ou $f = \{(a, b), (b, a), (c, d), (d, c)\}$.

14.80 (*a*) Veja a Figura 14-29. (*b*) 1, 2, 3, 4, 5. Os átomos são 2, 3 e 5. (*c*) 2 não tem nenhum, 10 tem 3.

(*d*) $60 = 4 \vee 3 \vee 5$, $30 = 2 \vee 3 \vee 5$, $20 = 4 \vee 5$; $15 = 3 \vee 5$, $12 = 3 \vee 4$, $10 = 2 \vee 5$, $6 = 2 \vee 3$.

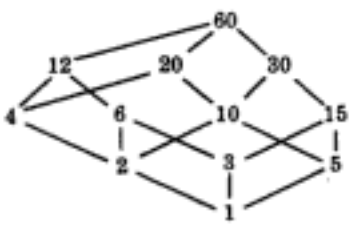


Fig. 14-29

Hidden page

Capítulo 15

Álgebra Booleana

15.1 INTRODUÇÃO

Conjuntos e proposições satisfazem leis similares que estão listadas nas Tabelas 1-1 e 4-1 (nos Capítulos 1 e 4, respectivamente). Essas leis são usadas para definir uma estrutura matemática abstrata chamada de *álgebra booleana*, assim denominada em homenagem ao matemático George Boole (1813-1864).

15.2 DEFINIÇÕES BÁSICAS

Seja B um conjunto não vazio com duas operações binárias, + e *, uma operação unária, ', e dois elementos distintos, 0 e 1. Então, B é dito uma *álgebra booleana* se valem os seguintes axiomas, onde a, b, c são elementos quaisquer de B:

- $[\mathbf{B}_1]$ Leis de comutatividade:
  $(1a)\ a + b = b + a$ $\qquad$ $(1b)\ a * b = b * a$
- $[\mathbf{B}_2]$ Leis de distributividade:
  $(2a)\ a + (b * c) = (a + b) * (a + c)$ $\qquad$ $(2b)\ a * (b + c) = (a * b) + (a * c)$
- $[\mathbf{B}_3]$ Leis de identidade:
  $(3a)\ a + 0 = a$ $\qquad$ $(3b)\ a * 1 = a$
- $[\mathbf{B}_4]$ Leis dos complementos:
  $(4a)\ a + a' = 1$ $\qquad$ $(4b)\ a * a' = 0$

Por vezes, designaremos uma álgebra booleana por $(B, +, *, ', 0, 1)$ se quisermos enfatizar suas seis partes. Dizemos que 0 é o elemento *zero*, 1 é o elemento *unidade* e a' é o *complemento* de a. Normalmente, omitiremos o símbolo * e usaremos justaposição. Então, $(2b)$ é escrito $a(b + c) = ab + ac$, que é a identidade familiar para anéis e corpos. Entretanto, $(2a)$ fica $a + bc = (a + b)(a + c)$ que, certamente, não é uma identidade usual em álgebra.

As operações +, * e ' são chamadas, respectivamente, de soma, produto e complemento. Adotamos a convenção usual de que, a menos que a parentetização indique precedência distinta, ' tem precedência sobre *, e * tem precedência sobre +. Por exemplo,

$a + b * c$ significa $a + (b * c)$, e não $(a + b) * c$ $\qquad$ $a * b'$ significa $a * (b')$, e não $(a * b)'$

Obviamente quando $a + b * c$ é escrito como $a + bc$, o significado é claro.

Exemplo 15.1

(*a*) Seja $\mathbf{B} = \{0,1\}$, o conjunto de *bits* (*binary digits*), com as operações binárias de + e * e a operação unária ′ definidas pela Figura 15-1. Então, **B** é uma álgebra booleana. (Note que ′ simplesmente muda o *bit*, i.e., $1' = 0$ e $0' = 1$.)

+	1	0
1	1	1
0	1	0

*	1	0
1	1	0
0	0	0

′	
1	0
0	1

Fig. 15-1

(*b*) Seja $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \cdots \times \mathbf{B}$ (n fatores) onde as operações de +, * e ′ são definidas componente a componente usando a Figura 15-1. Por conveniência de notação, escrevemos os elementos de $\mathbf{B}^n$ como seqüências de n *bits* sem vírgulas, por exemplo, $x = 110011$ e $y = 111000$ pertencem a $\mathbf{B}^6$. Portanto,

$$x + y = 111011, \qquad x * y = 110000, \qquad x' = 001100$$

*

Então, $\mathbf{B}^n$ é uma álgebra booleana. Aqui $0 = 000\ldots0$ é o elemento 0 e $1 = 111\ldots1$ é o elemento unidade. Observamos que $\mathbf{B}^n$ tem 2^n elementos.

(*c*) Seja $\mathbf{D}_{70} = \{1, 2, 5, 7, 10, 14, 35, 70, \}$, os divisores de 70. Defina +, * e ′ em $\mathbf{D}_{70}$ por

$$a + b = \text{mmc}(a, b), \qquad a * b = \text{mdc}(a, b), \qquad a' = \frac{70}{a}$$

Então, $\mathbf{D}_{70}$ é uma álgebra booleana onde 1 é o elemento zero e 70 é o elemento unidade.

(*d*) Seja $\mathcal{C}$ a coleção de conjuntos fechada sob as operações de união, interseção e complementos. Então, $\mathcal{C}$ é uma álgebra booleana onde o conjunto vazio, $\emptyset$, é o elemento zero, e o conjunto universo, U, é o elemento unidade.

Subálgebras, Álgebras Booleanas Isomorfas

Suponha que C é um subconjunto não vazio de uma álgebra booleana B. Dizemos que C é uma *subálgebra* de B se C é, em si, uma álgebra booleana (considerando as operações de B). Notamos que C é uma subálgebra de B se e somente se C é fechado sob as operações de B, i.e., +, * e ′. Por exemplo, {1, 2, 35, 70} é uma subálgebra de $\mathbf{D}_{70}$ no Exemplo 15.1(*c*).

Duas álgebras booleanas B e B' são ditas *isomorfas* se existe uma correspondência um-a-um que preserva as três operações, i.e., tal que

$$f(a + b) = f(a) + f(b), \qquad f(a * b) = f(a) * f(b) \qquad \text{e} \qquad f(a') = f(a)'$$

para quaisquer elementos a, b em B.

15.3 DUALIDADE

A dual de qualquer declaração em uma álgebra booleana B é a declaração obtida pela troca das operações + e * e de seus elementos identidade, 0 e 1, na declaração original. Por exemplo, o dual de

$$(1 + a) * (b + 0) = b \qquad \text{é} \qquad (0 * a) + (b * 1) = b$$

Observe a simetria dos axiomas em uma álgebra booleana B. Isto é, o dual do conjunto dos axiomas de B é o próprio conjunto de axiomas. Conseqüentemente, vale o importante princípio de dualidade em B. Esse princípio é enunciado como:

Teorema 15-1: (**Princípio da dualidade**) o dual de qualquer teorema em uma álgebra booleana também é um teorema.

Em outras palavras, se qualquer declaração é uma conseqüência dos axiomas de uma álgebra booleana, então a declaração dual também é uma conseqüência dos axiomas, já que pode ser provada usando o dual de cada passo da demonstração da declaração original.

15.4 TEOREMAS BÁSICOS

Usando os axiomas $[\mathbf{B}_1]$ a $[\mathbf{B}_4]$, provamos (Problema 15.5) o teorema seguinte.

Teorema 15-2: sejam a, b e c elementos em uma álgebra booleana B.

(i) Leis de idempotência

$(5a)$ $a + a = a$ $\qquad$ $(5b)$ $a * a = a$

(ii) Leis de limitação

$(6a)$ $a + 1 = 1$ $\qquad$ $(6b)$ $a * 0 = 0$

(iii) Leis de absorção

$(7a)$ $a + (a * b) = a$ $\qquad$ $(7b)$ $a * (a + b) = a$

(iv) Leis de associatividade

$(8a)$ $(a + b) + c = a + (b + c)$ $\qquad$ $(8b)$ $(a * b) * c = a * (b * c)$

O Teorema 15.2 e os nossos axiomas não contêm ainda todas as propriedades dos conjuntos listados na Tabela 1-1. Os dois próximos teoremas apresentam as outras propriedades.

Teorema 15-3: seja a um elemento qualquer de uma álgebra booleana B.

(i) (Unicidade do complemento) se $a + x = 1$ e $a * x = 0$, então $x = a'$.

(ii) (Lei de involução) $(a')' = a$.

(iii) $(9a)\ 0' = 1$. $\quad (9b)\ 1' = 0$.

Teorema 15-4 **(Leis de DeMorgan):** $(10a)$ $(a + b)' = a' * b'$. $\quad (10b)$ $(a * b)' = a' + b'$.

Provamos estes teoremas nos Problemas 15.6 e 15.7.

15.5 ÁLGEBRAS BOOLEANAS COMO RETICULADOS

Pelo Teorema 15.2 e pelo axioma $[\mathbf{B}_1]$, toda álgebra booleana B satisfaz as leis associativa, comutativa e de absorção e, portanto, é um reticulado onde $+$ e $*$ são as operações de disjunção e conjunção, respectivamente. Com relação a este reticulado, $a + 1 = 1$ implica $a \leq 1$ e $a * 0 = 0$ implica $0 \leq a$, para qualquer elemento $a \in B$. Portanto, B é um reticulado limitado. Além disso, os axiomas $[\mathbf{B}_2]$ e $[\mathbf{B}_4]$ mostram que B também é distributiva e complementada. Conversamente, todo reticulado L limitado, distributivo e complementado satisfaz os axiomas $[\mathbf{B}_1]$ a $[\mathbf{B}_4]$. Conseqüentemente, temos o resultado a seguir.

Definição alternativa: uma álgebra booleana B é um reticulado limitado, complementado e distributivo.

Como uma álgebra booleana B é um reticulado, tem uma ordem parcial natural (e assim, seu diagrama pode ser desenhado). Lembre (Capítulo 14) que definimos $a \leq b$ quando as condições equivalentes $a + b = b$ e $a * b = a$ valem. Como estamos trabalhando em uma álgebra booleana, de fato podemos afirmar mais.

Teorema 15-5: em uma álgebra booleana, as seguintes afirmativas são equivalentes:

$$(1)\quad a + b = b, \qquad (2)\quad a * b = a, \qquad (3)\quad a' + b = 1, \qquad (4)\quad a * b' = 0$$

Portanto, em uma álgebra booleana, podemos escrever $a \leq b$ sempre que se souber que qualquer uma das quatro condições acima é verdadeira.

Exemplo 15.2

(*a*) Considere uma álgebra booleana de conjuntos. Então, A precede o conjunto B se A é um subconjunto de B. O Teorema 15.4 afirma que, se $A \subseteq B$, como ilustrado no diagrama de Venn da Figura 15-2, valem as seguintes condições:

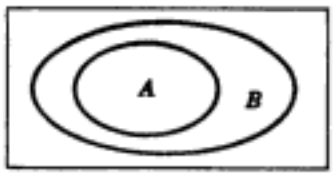
(1) $A \cup B = B$. $\qquad$ (3) $A^c \cup B = U$.

(2) $A \cap B = A$. $\qquad$ (4) $A \cap B^c = \varnothing$.

(*b*) Considere os booleanos $\mathbf{D}_N$. Então, a precede b se a divide b. Neste caso, mmc $(a, b) = b$ e mdc$(a, b) = a$. Por exemplo, seja $a = 2$ e $b = 14$. Então, valem as seguintes condições:

(1) $\text{mmc}(2, 14) = 14$. $\qquad$ (3) $\text{mmc}(2', 14) = \text{mmc}(35, 14) = 70$.

(2) $\text{mdc}(2, 14) = 2$. $\qquad$ (4) $\text{mdc}(2, 14') = \text{mdc}(2, 5) = 1$.



A é um subconjunto de B.

Fig. 15-2

15.6 TEOREMA DA REPRESENTAÇÃO

Seja B uma álgebra booleana finita. Lembre (Seção 14-9) que um elemento a em B é um átomo se a sucede 0 imediatamente, isto é, $0 \ll a$. Seja A o conjunto de átomos de B e seja $P(A)$ a álgebra booleana de todos os subconjuntos do conjunto de átomos A. Pelo Teorema 14.8, cada $x \neq 0$ em B pode ser expresso de maneira única (exceto pela ordem) como a soma (disjunção) de átomos, i.e., elementos de A. Digamos que

$$x = a_1 + a_2 + \cdots + a_r$$

é uma tal representação. Considere a função f: $B \to P(A)$ definida por

$$f(x) = \{a_1, a_2, \ldots, a_r\}$$

O mapeamento é bem definido, já que a representação é única.

Teorema 15-6: o mapeamento acima f: $B \to P(A)$ é um isomorfismo.

Assim, vemos o íntimo relacionamento entre a teoria dos conjuntos e as álgebras booleanas abstratas no sentido de que toda álgebra booleana finita é, estruturalmente, isomorfa à álgebra booleana de conjuntos.

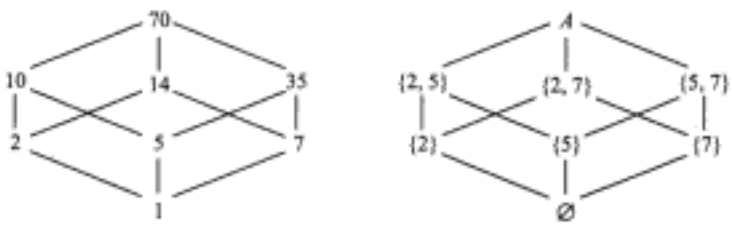
Se um conjunto A tem n elementos, o conjunto de suas partes, $P(A)$, tem 2^n elementos. Logo, o teorema acima nos fornece o próximo resultado.

Corolário 15-7: uma álgebra booleana finita tem 2^n elementos para algum inteiro positivo n.

Exemplo15.3 Considere a álgebra booleana $\mathbf{D}_{70} = \{1, 2, 5, \ldots, 70\}$ cujo diagrama está na Figura 15-3(a). Note que $A = \{2, 5, 7\}$ é o conjunto de átomos de $\mathbf{D}_{70}$. A seguinte representação de cada não-átomo em átomos é única.

$$10 = 2 \vee 5, \qquad 14 = 2 \vee 7, \qquad 35 = 5 \vee 7, \qquad 70 = 2 \vee 5 \vee 7$$

A Figura 15-3(b) apresenta o diagrama da álgebra booleana do conjunto $P(A)$ das partes do conjunto A de átomos. Observe que os dois diagramas são estruturalmente iguais.



(a) $\mathbf{D}_{70}$ (b) $P(A)$

Fig. 15-3

Hidden page

Diz-se que um produto fundamental P_1 *está contido em* (ou *incluído em*) outro produto fundamental P_2 se os literais de P_1 também são literais de P_2. Por exemplo, $x'z$ está contido em $x'yz$, mas $x'z$ não está contido em $xy'z$, já que x' não é um literal de $xy'z$. Observe que, se P_1 estiver contido em P_2, digamos, $P_2 = P_1 * Q$, pela lei da absorção,

$$P_1 + P_2 = P_1 + P_1 * Q = P_1$$

Logo, por exemplo, $x'z + x'yz = x'z$.

Definição: uma expressão booleana E é dita uma expressão em *soma de produtos* se E é um produto fundamental ou a soma de dois ou mais produtos fundamentais, onde um não está contido no outro.

Definição: seja E uma expressão booleana. Uma forma de E em *soma de produtos* é uma expressão em soma de produtos equivalente a E.

Exemplo 15.4 Considere a expressão

$$E_1 = xz' + y'z + xyz' \quad \text{e} \quad E_2 = xz' + x'yz' + xy'z$$

Embora a primeira expressão E_1 seja uma soma de produtos, não é uma expressão em soma de produtos. Especificamente, o produto xz' está contido no produto xyz'. Entretanto, pela lei de absorção, E_1 pode ser expressa como

$$E_1 = xz' + y'z + xyz' = xz' + xyz' + y'z = xz' + y'z$$

Isso leva a uma forma de E_1 em soma de produtos. A segunda expressão E_2 já é uma expressão em soma de produtos.

Algoritmo para Achar Formas de Soma de Produtos

O algoritmo de quatro passos, a seguir, usa as leis de álgebra booleana para transformar qualquer expressão booleana E em uma expressão equivalente na forma de soma de produtos.

Algoritmo 15.8A: a entrada é uma expressão booleana E. A saída é uma expressão equivalente em soma de produtos.

Passo 1 Use as leis de DeMorgan e involução para colocar a operação de complemento dentro de parênteses, até que a operação de complemento só seja aplicada a variáveis. Assim, E consistirá apenas em somas e produtos de literais.

Passo 2 Use a operação de distributividade para transformar E em uma soma de produtos.

Passo 3 Use as leis de comutatividade, idempotência e complementos para transformar cada produto em E em um produto fundamental ou 0.

Passo 4 Use as leis de absorção e identidade para, finalmente, transformar E em uma expressão em soma de produtos.

Exemplo 15.5 Suponha que o Algoritmo 15.8A seja aplicado à expressão booleana seguinte:

$$E = ((xy)'z)'((x' + z)(y' + z'))'$$

Passo 1 Usando as leis de involução e de DeMorgan, obtemos

$$E = (xy'' + z')((x' + z)' + (y' + z')') = (xy + z')(xz' + yz)$$

Agora E consiste em apenas somas e produtos de literais.

Passo 2 Usando as leis de distributividade obtemos

$$E = xyxz' + xyyz + xz'z' + yzz'$$

Passo 3 Usando as leis de comutatividade, idempotência e complementos, obtemos

$$E = xyz' + xyz + xz' + 0$$

Cada termo em E agora é um produto fundamental ou 0.

Passo 4 O produto ac' está contido em abc'; portanto, pela lei de absorção,

$$xz' + (xz' * y) = xz'$$

Logo, podemos deletar abc' da soma. Além disso, pela lei de identidade para 0, podemos deletar 0 da soma. Conseqüentemente,

$$E = xyz + xz'$$

E fica assim representado como uma expressão em soma de produtos.

Formas Completas em Soma de Produtos

Uma expressão booleana $E = E(x_1, x_2, \ldots, x_n)$ é dita uma expressão em *soma de produtos completa* se E é uma expressão em soma de produtos, onde cada produto P envolve todas as n variáveis. Pode-se usar o teorema seguinte.

Teorema 15-8: toda expressão booleana diferente de zero $E = E(x_1, x_2, \ldots, x_n)$ é equivalente a uma expressão em soma de produtos completa, e esta representação é única.

A representação única de E mencionada acima é denominada *forma completa em soma de produtos* de E. Lembre que o Algoritmo 15.8A nos diz como transformar E na forma de soma de produtos. O algoritmo seguinte mostra como transformar uma forma de soma de produtos em uma forma completa de soma de produtos.

Algoritmo 15.8B: a entrada é uma expressão booleana $E = E(x_1, x_2, \ldots, x_n)$ na forma de soma de produtos. A saída é uma expressão completa em soma de produtos equivalente a E.

Passo 1 Ache um produto P em E que não envolva a variável x_i e multiplique P por $x_i + x_i'$, deletando produtos repetidos. (Isto é possível porque $x_i + x_i' = 1$, e $P + P = 1$.)

Passo 2 Repita o Passo 1 até que todo produto P seja um termo completo[†], isto é, todo produto P envolva todas as variáveis.

Exemplo 15.6 Expresse $E(x, y, z) = x(y'z)'$ na sua forma completa de soma de produtos.

(*a*) Use o Algoritmo 18.5A em E para obter

$$E = x(y'z)' = x(y + z') = xy + xz'$$

(*b*) Use o Algoritmo 18.5B em E para obter

$$\begin{aligned} E &= xy(z + z') + xz'(y + y') = xyz + xyz' + xyz' + xy'z' \\ &= xyz + xyz' + xy'z' \end{aligned}$$

Agora E está representada pela sua forma completa em soma de produtos.

Aviso: a terminologia desta seção não está padronizada. A forma em soma de produtos para uma expressão booleana E também é chamada de *forma disjuntiva normal* ou FDN de E. A forma em soma de produtos completa é também chamada de *forma disjuntiva normal completa*, ou *forma canônica disjuntiva* de E.

15.9 EXPRESSÕES BOOLEANAS MINIMAIS E IMPLICANTES PRIMOS

Existem muitas maneiras de representar a mesma expressão booleana E. Definimos e investigamos aqui uma forma minimal para E em soma de produtos. Precisamos também definir e investigar implicantes primos, de E[††] pois a forma minimal em soma de produtos envolve implicantes primos. Existem outras formas minimais, mas seu estudo vai além dos objetivos deste texto.

[†] N. de T. No original, *minterm*.

[††] N. de T. No original, *prime implicants*. A tradução deste termo não está padronizada. Por uma questão de compatibilidade, optamos por usar aqui o termo que aparece em algumas grades curriculares de disciplinas de circuitos lógicos.

Soma de Produtos em Forma Minimal

Considere uma expressão booleana E em forma de soma de produtos. Seja E_L o número de literais em E (incluindo multiplicidade na contagem). Por exemplo, suponha que

$$E = xyz' + x'y't + xy'z't + x'yzt$$

Então, $E_L = 3 + 3 + 4 + 4 = 14$ e $E_S = 4$.

Suponha que E e F são expressões booleanas equivalentes na forma de soma de produtos. Dizemos que E é *mais simples* do que F se

$$\text{(i)} \quad E_L < F_L \quad \text{e} \quad E_S \leq F_L, \qquad \text{ou} \qquad \text{(ii)} \quad E_L \leq F_L \quad \text{e} \quad E_S < F_L$$

Dizemos que E é *minimal* se não existe expressão equivalente em forma de soma de produtos que seja mais simples do que E. Observamos que pode haver mais do que uma expressão equivalente minimal de soma de produtos.

Implicantes Primos

Um produto fundamental P é dito um *implicante primo* de uma expressão booleana se

$$P + E = E$$

e nenhum outro produto fundamental contido em P tem esta propriedade. Por exemplo, suponha que

$$E = xy' + xyz' + x'yz'$$

Pode-se mostrar (Problema 15.15) que

$$xz' + E = E \qquad \text{mas} \qquad x + E \neq E \qquad \text{e} \qquad z' + E \neq E$$

Logo, xz' é um implicante primo de E.

O seguinte teorema pode ser usado.

Teorema 15-9: uma forma minimal em soma de produtos de uma expressão booleana E é uma soma de implicantes primos de E.

As subseções seguintes apresentam um método para se achar implicantes primos de E baseado na noção de *consensus* de produtos fundamentais. Este método pode ser então usado para achar uma forma minimal em soma de produtos de E. A Seção 15.2 apresenta um método geométrico para achar esses implicantes primos.

Consensus de Produtos Fundamentais

Sejam P_1 e P_2 produtos fundamentais tais que exatamente uma variável, digamos, x_k, aparece sem complementos em um deles, P_1 ou P_2, e complementada no outro. Então, o *consensus* de P_1 e P_2 é o produto (sem repetições) dos literais de P_1 e dos literais de P_2 após a deleção de x_k e x_k'. (Não definimos o *consensus* de $P_1 = x$ e $P_2 = x'$.)

O lema seguinte (provado no Problema 15.19) pode ser usado.

Lema 15.10: suponha que Q o *consensus* de P_1 e P_2. Então, $P_1 + P_2 + Q = P_1 + P_2$.

Exemplo 15.7 Ache o *consensus* Q de P_1 e P_2 onde:

(*a*) $P_1 = xyz's$ e $P_2 = xy't$.

Delete y e y' e depois multiplique os literais de P_1 e P_2 (sem repetições) para obter $Q = xz'st$.

(*b*) $P_1 = xy'$ e $P_2 = y$.

Deletando y e y', obtém-se $Q = x$.

(*c*) $P_1 = x'yz$ e $P_2 = x'yt$.

Nenhuma variável aparece não complementada em algum dos produtos e com complemento no outro. Logo, P_1 e P_2 não têm *consensus*.

(*d*) $P_1 = x'yz$ e $P_2 = xyz'$.

Tanto x quanto z aparecem complementadas em um produto.

Método do *Consensus* para Determinar Implicantes Primos

O algoritmo seguinte, conhecido como *método do consensus*, é usado para determinar os implicantes primos de uma expressão booleana.

Algoritmo 15.9A: (**Método do *consensus***) a entrada é uma expressão booleana $E = P_1 + P_2 + \cdots + P_m$ onde os P são produtos fundamentais. A saída expressa E como uma soma de seus implicantes primos (Teorema 15.11).

Passo 1 Delete qualquer produto fundamental P_i que inclua qualquer outro produto fundamental P_j. (É permitido pela lei da absorção.)

Passo 2 Adicione o *consensus* de quaisquer P_i e P_j desde que Q não inclua nenhum dos Ps. (É permitido pelo Lema 15.10.)

Passo 3 Repita o Passo 1 e/ou o Passo 2 até que nenhum dos dois seja mais possível.

O teorema seguinte enuncia as propriedades básicas do algoritmo acima.

Teorema 15-11: o método de *consensus* irá terminar e, então, E será a soma de seus implicantes primos.

Exemplo 15.8 Seja $E = xyz + x'z' + xyz' + x'y'z + x'yz'$. Então,

$$\begin{aligned}
E &= xyz + x'z' + xyz' + x'y'z && (x'yz' \text{ inclui } x'z') \\
&= xyz + x'y' + xyz' + x'y'z + xy && (\textit{consensus} \text{ de } xyz \text{ e } xyz') \\
&= x'z' + x'y'z + xy && (xyz \text{ and } xyz' \text{ inclui } xy) \\
&= x'z' + x'y'z + xy + x'y' && (\textit{consensus} \text{ de } x'z' \text{ e } x'y'z) \\
&= x'z' + xy + x'y' && (x'y'z \text{ inclui } x'y') \\
&= x'z' + xy + x'y' + yz' && (\textit{consensus} \text{ de } x'z' \text{ e } xy)
\end{aligned}$$

A partir de agora, nenhum passo no método de *consensus* irá mudar E. Logo, E é a soma de seus implicantes primos, que aparecem na última linha, isto é, $x'z'$, xy, $x'y'$ e yz'.

Achando uma Forma Minimal em Soma de Produtos

O método do *consensus* (Algoritmo 15.9A) pode ser usado para expressar uma expressão booleana E como a soma de seus implicantes primos. Usando uma tal soma, pode-se achar uma forma minimal em soma de produtos para E como a seguir.

Algoritmo 15.9B: a entrada é uma expressão booleana $E = P_1 + P_2 + \cdots + P_m$ onde os P são todos os implicantes primos de E. A saída expressa E como uma soma de produtos minimal.

Passo 1 Expresse cada implicante primo P como uma soma de produtos completa.

Passo 2 Delete, um por um, todos os implicantes primos cujos termos na soma aparecem entre as parcelas da soma dos implicantes primos restantes.

Exemplo 15.9 Aplicamos o Algoritmo 15.9B para

$$E = x'z' + xy + x'y' + yz'$$

(Pelo Exemplo 15.8, E fica agora expresso como a soma de todos os seus implicantes primos.)

Passo 1 Expresse cada implicante primo de E como uma soma de produtos completa para obter

$$\begin{aligned}
x'z' &= x'z'(y + y') = x'yz' + x'y'z' \\
xy &= xy(z + z') = xyz + xyz' \\
x'y' &= x'y'(z + z') = x'y'z + x'y'z' \\
yz' &= yz'(x + x') = xyz' + x'yz'
\end{aligned}$$

Passo 2 Os termos na soma de $x'z'$ que aparecem entre outros termos de soma são $x'yz$ e $x'y'z'$. Logo, delete $x'y'$ para obter

$$E = xy + x'y' + yz'$$

As parcelas de qualquer outro implicante primo não aparecem entre as parcelas dos implicantes primos remanescentes e, portanto, esta é uma forma minimal em soma de produtos de E. Em outras palavras, nenhum dos implicantes primos remanescentes é supérfluo, isto é, nenhum deles pode ser deletado sem que se altere E.

15.10 PORTAS LÓGICAS E CIRCUITOS

Circuitos lógicos (também chamados *redes lógicas*) são estruturas construídas a partir de certos circuitos elementares chamados *portas lógicas*. Cada circuito lógico pode ser visto como uma máquina L que contém um ou mais dispositivos de entrada e exatamente um dispositivo de saída. Cada dispositivo de entrada em L manda um sinal, especificamente, um *bit*

$$0 \quad \text{ou} \quad 1$$

ao circuito L, e L processa o conjunto de *bits* para obter um *bit* de saída. Conseqüentemente, uma seqüência de n *bits* pode ser associada a cada dispositivo de entrada, e L processa as seqüências de entrada, um *bit* a cada vez, para produzir uma seqüência de saída de n *bits*. Primeiramente definimos as portas lógicas, e depois investigamos os circuitos lógicos.

Portas Lógicas

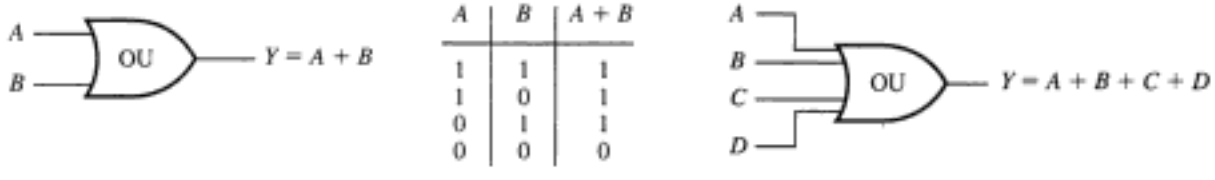
Existem três tipos básicos de portas lógicas, que estão descritos abaixo. Adotamos a convenção de que as linhas que entram à esquerda no símbolo de porta são linhas de entrada, e a linha única que sai à direita é a linha de saída.

(*a*) ***Porta OU***: a Figura 15-5(*a*) mostra uma porta OU com entradas A e B e saída $Y = A + B$, onde a "adição" é definida pela "tabela-verdade" da Figura 15-5(*b*). Assim, a saída é $Y = 0$ apenas quando as entradas são $A = 0$ e $B = 0$. Uma porta do tipo OU pode ter mais de duas entradas. A Figura 15-5(*c*) mostra uma porta do tipo OU com quatro entradas, A, B, C e D, e saída $Y = A + B + C + D$. A saída é $Y = 0$ se e somente se todas as entradas são 0.

Suponha, por exemplo, que os dados de entrada para a porta OU da Figura 15-5(*c*) são as seguintes seqüências de oito *bits*:

$$A = 10000101, \qquad B = 10100001, \qquad C = 00100100, \qquad D = 10010101$$

A porta OU só produzirá 0 quando todos os *bits* de entrada forem 0. Isso só ocorre nas segunda, quinta e sétima posições (lendo da esquerda para a direita). Portanto, a saída é a seqüência $Y = 10110101$.



(*a*) Porta OU (*b*) (*c*)

Fig. 15-5

(*b*) ***Porta E***: a Figura 15-6(*a*) mostra uma porta E com entradas A e B e saídas $Y = A \cdot B$ (ou, simplesmente, $Y = AB$), onde a "multiplicação" é definida pela "tabela-verdade" da Figura 15-6(*b*). Assim, a saída é $Y = 1$ quando as entradas são $A = 1$ e $B = 1$; caso contrário, $Y = 0$. Uma porta E pode ter mais do que duas entradas. A Figura 15-6(*c*) mostra uma porta E com quatro entradas, A, B, C e D, e saída $Y = A \cdot B \cdot C \cdot D$. A saída é $Y = 1$ se e somente se todas as entradas são 1.

Suponha, por exemplo, que os dados de entrada para a porta E da Figura 15-6(*c*) sejam as seguintes seqüências de oito *bits*:

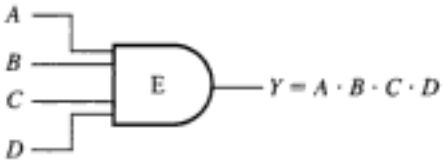
$$A = 11100111, \qquad B = 01111011, \qquad C = 01110011, \qquad D = 11101110$$

A porta E produzirá 1 apenas se todos os *bits* de entrada forem iguais a 1. Isto só ocorre nas segunda, terceira e sétima posições. Logo, a seqüência de saída é $Y = 01100010$.

(*a*) Porta E

A	B	$A \cdot B$
1	1	1
1	0	0
0	1	0
0	0	0

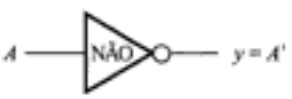
(*b*)



(*c*)

Fig. 15-6

(*c*) ***Porta NÃO***: a Figura 15-7(*a*) mostra uma porta NÃO, também chamada de *inversor*, com entrada A e saída $Y = A'$, onde "inversão", denotada por ', é definida pela "tabela-verdade" da Figura 15-7(*b*). O valor da saída $Y = A'$ é o oposto da entrada A; isto é, $A' = 1$ quando $A = 0$ e $A' = 0$ quando $A = 1$. Enfatizamos que uma porta NÃO só pode ter uma entrada, enquanto as portas E e OU podem ter duas ou mais entradas.



(*a*) Porta NÃO

A	A'
1	0
0	1

(*b*)

Fig. 15-7

Suponha, por exemplo, que uma porta NÃO deve processar as três seqüências seguintes:

$$A_1 = 110001, \qquad A_2 = 10001111, \qquad A_3 = 101100111000$$

A porta NÃO muda 0 para 1 e 1 para 0. Logo,

$$A_1' = 001110, \qquad A_2' = 01110000, \qquad A_3' = 010011000111$$

são as três saídas correspondentes.

Circuitos Lógicos

Um circuito lógico L é uma estrutura bem formada cujos componentes elementares são as portas OU, E e NÃO acima descritas. A Figura 15-8 é um exemplo de um circuito lógico com entradas A, B e C e saída Y. Um ponto indica um local onde a linha de entrada se divide de maneira tal que o sinal enviado pelo *bit* é emitido em mais de uma direção. (Por conveniência de notação, freqüentemente, omitimos a palavra no interior do símbolo de porta.) Trabalhando da esquerda para a direita, expressamos Y em termos das entradas A, B e C como a seguir. A saída da porta E é $A \cdot B$, que é, então, anulado para produzir $(A \cdot B)'$. A saída da porta OU mais baixa é $A' + C$, que é, então, anulado para obter $(A' + C)'$. A saída da porta OU mais à direita, com entrada $(A \cdot B)'$ e $(A' + C)'$, nos dá a representação desejada, isto é,

$$Y = (A \cdot B)' + (A' + C)'$$

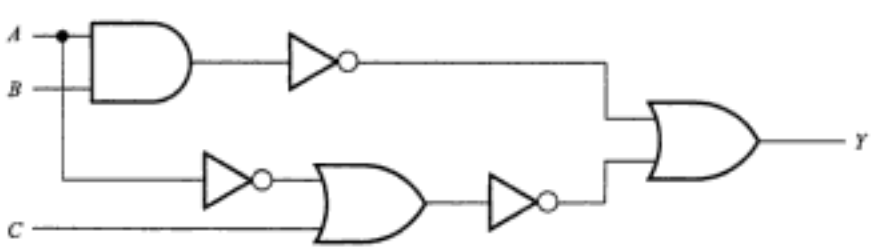


Fig. 15-8

Circuitos Lógicos e Álgebras Booleanas

Observe que as tabelas-verdade para as portas OU, E e NÃO são, respectivamente, idênticas às tabelas-verdade para as proposições $p \vee q$ (disjunção "p ou q"), $p \wedge q$ (conjunção "p e q"), e $\neg p$ (negação, "não p"), que aparecem na Seção 4.3. A única diferença é que são usados 1 e 0 no lugar de V e F. Logo, os circuitos lógicos satisfazem as mesmas leis que as proposições e, portanto, formam uma álgebra booleana. Declaramos este resultado formalmente.

Teorema 15-12: Circuitos lógicos formam uma álgebra booleana.

Conseqüentemente, todos os termos utilizados em álgebras booleanas, tais como complementos, literais, produtos fundamentais, e soma de produtos completa, também podem ser usados nos nossos circuitos lógicos.

Circuitos E-OU

O circuito lógico L, que corresponde a uma expressão booleana em soma de produtos, é denominado um circuito E-OU. Um circuito L como este tem várias entradas, onde:

(1) Algumas das entradas ou seus complementos alimentam cada uma das portas E.
(2) As saídas de todas as portas E alimentam uma única porta OU.
(3) A saída da porta OU é a saída do circuito L.

A ilustração deste tipo de circuito lógico está feita a seguir.

Exemplo 15.10 A Figura 15-9 é um típico circuito E-OU com três entradas A, B e C e saída Y. Podemos facilmente expressar Y como uma expressão booleana nas entradas A, B e C como a seguir. Achamos primeiramente a saída de cada porta E:

(*a*) As entradas da primeira porta E são A, B e C; portanto, $A \cdot B \cdot C$ é a saída.
(*b*) As entradas da segunda porta E são A, B' e C; portanto, $A \cdot B' \cdot C$ é a saída.
(*c*) As entradas da terceira porta E são A' e B; portanto, $A' \cdot B$ é a saída.

Então, a soma das saídas das portas E é a saída da porta OU, que é a saída Y do circuito. Logo,

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

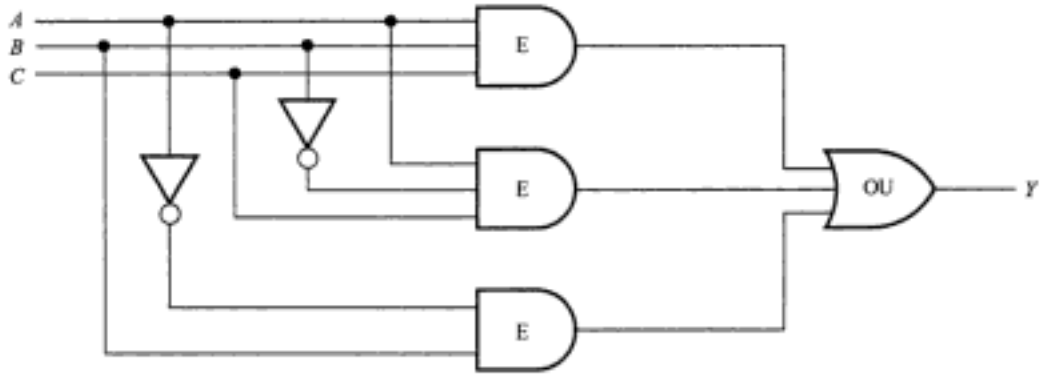


Fig. 15-9

Portas NE e NOU

Existem duas portas adicionais, equivalentes a combinações das portas básicas referidas acima.

(*a*) Uma porta NE, representada na Figura 15-10(*a*), é equivalente a uma porta E seguida por uma porta NÃO.
(*b*) Uma porta NOU representada na Figura 15-10(*a*), é equivalente a uma porta OU seguida por uma porta NÃO.

As tabelas-verdade para estas portas (usando duas entradas A e B) aparecem na Figura 15-10(*c*). As portas NE e NOU podem, na verdade, ter duas ou mais entradas, exatamente como suas portas correspondentes E e OU. Além disso, a saída de uma porta NE é 0 se e somente se todas as entradas são 1, e a saída de uma porta NOU é 1 se e somente se todas as entradas são 0.

(*a*) Porta NE

(*b*) Porta NOU

A	*B*	NE	NOU
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

(*c*)

Fig. 15-10

Observe que a única diferença entre as portas E e NE e OU e NOU é que as portas NE e NOU são seguidas por um círculo. Alguns textos também usam este círculo para indicar um complemento antes de uma porta. Por exemplo, a expressões booleanas correspondente aos dois circuitos lógicos da Figura 15-11 são

$$(a) \quad Y = (A'B)', \qquad (b) \quad Y = (A' + B' + C)'$$

(*a*)

(*b*)

Fig. 15-11

15.11 TABELAS-VERDADE E FUNÇÕES BOOLEANAS

Considere um circuito lógico L com $n = 3$ dispositivos de entrada A, B e C e saída Y, digamos,

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

Cada atribuição de um conjunto de três *bits* às entradas A, B e C produz um *bit* de saída para Y. Juntando tudo, existem $2^n = 2^3 = 8$ maneiras possíveis para atribuir *bits* de entrada, como a seguir:

$$000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111$$

Supomos que a seqüência dos primeiros *bits* é atribuída a A, a seqüência dos segundos *bits* a B, e a seqüência dos terceiros *bits* a C. Portanto, o conjunto de entradas acima pode ser rescrito na forma

$$A = 00001111, \qquad B = 00110011, \qquad C = 01010101$$

Enfatizamos que estas três 2^n = seqüências de oito *bits* contêm as oito combinações possíveis de *bits* de entrada.

A *tabela-verdade* $T = T(L)$ do circuito L acima consiste na seqüência de saída Y que corresponde às seqüências de entrada A, B, C. Esta tabela-verdade T pode ser expressa usando notação fracional ou relacional, isto é, pode ser escrita na forma

$$T(A, B, C) = Y \qquad \text{ou} \qquad T(L) = [A, B, C; Y]$$

Essa forma para a tabela-verdade de L é essencialmente a mesma que a tabela-verdade para as proposições discutida na Seção 4.4. A única diferença é que aqui os valores de A, B, C e Y são escritos no sentido horizontal enquanto na Seção 4.4 estão escritos verticalmente.

Considere um circuito lógico L com n dispositivos de entrada. Existem muitas maneiras de formar n seqüências de entrada $A_1, A_2, \ldots, A_n$ contendo as 2^n combinações possíveis de *bits* de entrada. (Note que cada seqüência deve conter 2^n *bits*.) Um esquema para atribuição é:

$\mathbf{A}_1$: Atribua 2^{n-1} *bits* 0s seguidos de 2^{n-1} *bits* 1s.
$\mathbf{A}_2$: Repetidamente, atribua 2^{n-2} *bits* 0s seguidos de 2^{n-2} *bits* 1s.
$\mathbf{A}_3$: Repetidamente, atribua 2^{n-3} *bits* 0s seguidos de 2^{n-3} *bits* 1s.

E assim sucessivamente. As seqüências obtidas desta forma serão chamadas *seqüências especiais*. A troca de 0 por 1 e 1 por 0 nas seqüências especiais produz os complementos das seqüências especiais.

Observação: Admitindo que a entrada são as seqüências especiais, freqüentemente não precisamos distinguir entre a tabela-verdade

$$T(L) = [A_1, A_2, \ldots, A_n; Y]$$

e a própria saída Y.

Exemplo 15.11

(*a*) Suponha que um circuito lógico L tenha $n = 4$ dispositivos de entrada A, B, C, D. As seqüências especiais de $2^n = 2^4 = 16$ *bits* para A, B, C e D são

$$A = 0000000011111111, \qquad C = 0011001100110011$$
$$B = 0000111100001111, \qquad D = 0101010101010101$$

Isto é:

(1) A começa com oito 0s seguidos de oito 1s. (Aqui, $2^{n-1} = 2^3 = 8$.)

(2) B começa com quatro 0s seguidos de quatro 1s, e assim por diante. (Aqui, $2^{n-2} = 2^2 = 4$.)

(3) C começa com dois 0s seguidos de dois 1s, e assim por diante. (Aqui, $2^{n-3} = 2^1 = 2$.)

(4) D começa com um 0 seguido de um 1, e assim por diante. (Aqui, $2^{n-4} = 2^0 = 1$.)

(*b*) Suponha que um circuito lógico L tenha $n = 3$ dispositivos de entrada A, B, C. As seqüências especiais de $2^n = 2^3 = 8$ *bits* para A, B, C, e seus complementos são

$$A = 00001111, \qquad B = 00110011, \qquad C = 01010101$$
$$A' = 11110000, \qquad B' = 11001100, \qquad C' = 10101010$$

Apresentamos a seguir um algoritmo de três passos para determinar a tabela-verdade para um circuito lógico L onde a saída Y é uma soma dada, na entrada, por uma expressão booleana em soma de produtos.

Algoritmo 15.11: a entrada é uma expressão booleana em forma de soma de produtos $Y = Y(A_1, A_2, \ldots)$.

Passo 1 Escreva as seqüências especiais para as entradas $A_1, A_2, \ldots$ e suas componentes.

Passo 2 Ache cada produto que aparece em Y. (Lembre que o produto $X_1 \cdot X_2 \cdots = 1$ em uma posição se e somente se todos os $X_1, X_2, \ldots$ tem 1 na mesma posição.)

Passo 3 Ache a soma Y dos produtos. (Lembre que o produto $X_1 + X_2 + \cdots = 0$ em uma posição se e somente se todos os $X_1, X_2, \ldots$ tem 0 na mesma posição.)

Exemplo 15.12 O Algoritmo 15.11 é usado para achar a tabela-verdade $T = T(L)$ do circuito lógico L na Figura 15-9 ou, equivalentemente, da expressão booleana em soma de produtos acima:

$$Y = A \cdot B \cdot C + A \cdot B' \cdot C + A' \cdot B$$

(1) As seqüências especiais e seus complementos aparecem no Exemplo 15.11(*b*).

(2) Os produtos são

$$A \cdot B \cdot C = 00000001, \qquad A \cdot B' \cdot C = 00000100, \qquad A' \cdot B = 00110000$$

(3) A soma é $Y = 00110101$.

Conseqüentemente,

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

ou, simplesmente, $T(L) = 00110101$, onde assumimos que a entrada consiste nas seqüências especiais.

Funções Booleanas

Seja E uma expressão booleana com n variáveis $x_1, x_2, \ldots, x_n$. Toda a discussão anterior pode também ser aplicada a E, onde, neste caso, as seqüências especiais são atribuídas às variáveis $x_1, x_2, \ldots, x_n$ em vez de o serem aos dispositivos de entrada $A_1, A_2, \ldots, A_n$. A tabela-verdade $T = T(E)$ de E é definida da mesma maneira que a tabela-verdade $T = T(L)$ para um circuito lógico L. Por exemplo, a expressão booleana

$$E = xyz + xy'z + x'y$$

que é análoga ao circuito lógico L do Exemplo 15.12, produz a tabela-verdade

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

ou, simplesmente, $T(E) = 00110101$, onde assumimos que a entrada consiste nas seqüências especiais.

Observação: A tabela-verdade para uma expressão booleana $E = E(x_1, x_2, \ldots, x_n)$ com n variáveis também pode ser encarada como uma função "booleana" de B^n para B. [As álgebras booleanas B^n e $B = \{0,1\}$ estão definidas no Exemplo 15.1.] Isto é, cada elemento em B^n é uma lista de n *bits* os quais, quando associados a uma lista de variáveis em E, produzem um elemento em B. A tabela-verdade $T(E)$ de E é, simplesmente, o gráfico da função.

Exemplo 15.13

(*a*) Considere a expressão booleana $E = E(x, y, z)$ com três variáveis. Os oito termos completos (produtos fundamentais envolvendo todas as três variáveis) são

$$xyz,\quad xyz',\quad xy'z,\quad x'yz,\quad xy'z',\quad x'yz',\quad x'y'z'$$

As tabelas-verdade para estes termos completos (usando as seqüências especiais para x, y e z) são:

$$xyz = 00000001,\quad xyz' = 00000010,\quad xy'z = 00000100,\quad x'yz = 00001000$$
$$xy'z' = 00010000,\quad x'yz' = 00100000,\quad x'y'z = 01000000,\quad x'y'z' = 10000000$$

Observe que cada termo completo assume o valor 1 em apenas uma das oito posições.

(*a*) Considere a expressão booleana $E = xyz' + x'yz + x'y'z$. Note que E é uma expressão completa em soma de produtos contendo três termos completos. Conseqüentemente, a tabela-verdade $T = T(E)$ para E, usando as seqüências especiais para x, y, z, pode ser facilmente obtidas a partir das seqüências na parte (*a*). Especificamente, a tabela-verdade $T(E)$ conterá exatamente três 1s na mesma posição dos 1s dos três termos completos em E. Logo,

$$T(00001111,\ 00110011,\ 01010101) = 01001010$$

ou, simplesmente, $T(E) = 01001010$.

15.12 MAPAS DE KARNAUGH

Os mapas de Karnaugh, nos quais os termos completos envolvendo as mesmas variáveis são representados por quadrados, são dispositivos pictóricos para determinar implicantes primos e formas minimais para expressões booleanas envolvendo, no máximo, seis variáveis. Trataremos apenas dos casos com duas, três e quatro variáveis. No contexto de mapas de Karnaugh, usaremos, às vezes, as expressões "quadrado" e "termo completo" indistintamente. Lembre que um termo completo é um produto fundamental que envolve todas as variáveis, e que uma expressão completa em soma de produtos é uma soma de termos completos.

Precisamos definir primeiramente a noção de produtos adjacentes. Dois produtos fundamentais, P_1 e P_2, são ditos *adjacentes* se P_1 e P_2 têm as mesmas variáveis e se diferem em exatamente um literal. Portanto, é necessário que existam uma variável não complementada em um produto e uma complementada no outro. Em particular, a soma de dois produtos adjacentes é um produto fundamental com um literal a menos.

Exemplo 15.14 Ache a soma de produtos adjacentes P_1 e P_2 onde:

(*a*) $P_1 = xyz'$ e $P_2 = xy'z'$.

$$P_1 + P_2 = xyz' + xy'z' = xz'(y + y') = xz'(1) = xz'$$

(*b*) $P_1 = x'yzt$ e $P_2 = x'yz't$.

$$P_1 + P_2 = x'yzt + x'yz't = x'yt(z + z') = x'yt(1) = x'yt$$

(*c*) $P_1 = x'yzt$ e $P_2 = xyz't$.

Aqui, P_1 e P_2 não são adjacentes, uma vez que diferem em dois literais. Em particular,

$$P_1 + P_2 = x'yzt + xyz't = (x' + x)y(z + z')t = (1)y(1)t = yt$$

(*d*) $P_1 = xyz'$ e $P_2 = xyzt$.

Aqui, P_1 e P_2 não são adjacentes, já que têm variáveis diferentes. Logo, em particular, eles não aparecerão como quadrados no mesmo mapa de Karnaugh.

O Caso de Duas Variáveis

O mapa de Karnaugh correspondente a expressões booleanas $E(x, y)$ de duas variáveis, x e y, é mostrado na Figura 15-12(*a*). O mapa de Karnaugh pode ser encarado como um diagrama de Venn onde x é representado pelos pontos na metade superior do mapa, sombreada na Figura 15-12(*b*), e y é representado pelos pontos na metade esquerda do mapa, sombreada na Figura 15-12(*c*). Logo, x' é representado pelos pontos na metade inferior do mapa e y' é representado pelos pontos na metade direita do mapa. Conseqüentemente, os quatro possíveis termos completos com dois literais

$$xy, \quad xy', \quad x'y, \quad x'y'$$

estão representados pelos quatro quadrados no mapa, como indicado na Figura 14-12(*d*). Note que dois destes quadrados são adjacentes, de acordo com a definição acima, se e somente se os quadrados são geometricamente adjacentes (têm um lado em comum).

(*a*) (*b*) *x* sombreado (*c*) *y* sombreado (*d*)

Fig. 15-12

Qualquer expressão booleana $E(x, y)$ em forma completa de soma de produtos é uma soma de termos completos e, portanto, pode ser representada no mapa de Karnaugh pela colocação de sinais do tipo "√" (visto) nos quadrados adequados. Um implicante primo de $E(x, y)$ será um par de quadrados adjacentes em E ou um quadrado *isolado*, i.e., um quadrado que não é adjacente a nenhum outro quadrado de $E(x,y)$. Uma forma minimal em soma de produtos para $E(x, y)$ consistirá em um número mínimo de implicantes primos cobrindo todos os quadrados de $E(x, y)$ como ilustrado no próximo exemplo.

Exemplo 15.15 Ache os implicantes primos e uma forma minimal em soma de produtos para cada uma das seguintes expressões booleanas completas em soma de produtos:

$$(a)\ E_1 = xy + xy'; \quad (b)\ E_2 = xy + x'y + x'y'; \quad (c)\ E_3 = xy + x'y'$$

Isso pode ser feito usando o mapa de Karnaugh como a seguir:

(*a*) Marque os quadrados correspondentes a xy e xy' como na Figura 15-13(*a*). Note que E_1 consiste em um implicante primo, os dois quadrados adjacentes identificados pelo laço na Figura 15-13(*a*). Este par de quadrados adjacentes representa a variável x; logo, x é um (o único) implicante primo de E_1. Conseqüentemente, $E_1 = x$ é sua soma minimal.

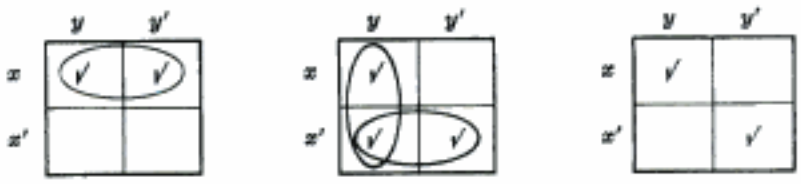


Fig. 15-13

(*b*) Marque os quadrados correspondentes a xy e $x'y'$ como na Figura 15-13(*a*). Note que E_2 contém dois pares de quadrados adjacentes (identificados pelos dois laços) que incluem todos os quadrados de E_2. O par vertical representa y e o par horizontal representa x'; portanto, y e x' são os implicantes primos de E_2. Logo, $E_2 = x' + y$ é sua soma minimal.

(*c*) Marque os quadrados correspondentes a xy e $x'y'$ como na Figura 15-13(c). Note que E_3 consiste em dois quadrados isolados que representam xy e $x'y'$; logo, xy e $x'y'$ são os implicantes primos de E_3, e $E_3 = xy + x'y'$ é sua soma minimal.

O Caso de Três Variáveis

O mapa de Karnaugh correspondente a uma expressão booleana $E = E(x, y, z)$ com três variáveis x, y e z é mostrado na Figura 15-14(*a*). Lembre que existem exatamente oito termos completos com três variáveis:

$$xyz, \quad xyz', \quad xy'z', \quad xy'z, \quad x'yz, \quad x'yz', \quad x'y'z', \quad x'y'z$$

Esses termos completos estão listados de tal modo que correspondem aos oito quadrados no mapa de Karnaugh, de maneira óbvia.

Além disso, a fim de que todo par de produtos adjacentes na Figura 15-14(*a*) seja geometricamente adjacente, as arestas direita e esquerda do mapa devem ser identificadas. Isto é equivalente a cortar, dobrar e colar o mapa ao longo das arestas identificadas para obter o cilindro desenhado na Figura 15-14(*b*), onde produtos adjacentes são, agora, representados por quadrados com um lado comum.

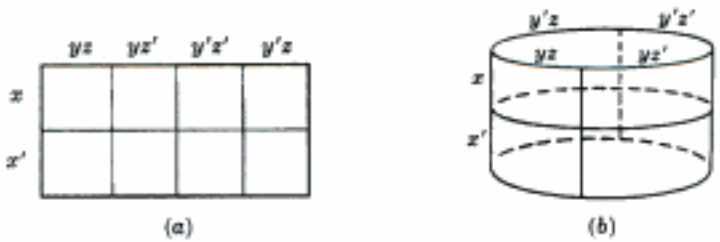


Fig. 15-14

Encarando o mapa de Karnaugh na Figura 15-14(*a*) como um diagrama de Venn, as áreas representando as variáveis x, y e z estão assinaladas na Figura 15-15. Especificamente, a variável x ainda é representada pelos pontos na metade superior do mapa, como sombreado na Figura 15-15(*a*), e a variável y ainda é representada pelos pontos na metade esquerda do mapa como indicado na Figura 15-15(*b*). A nova variável z é representada pelos pontos nas quartas partes esquerda e direita do mapa, como indicado na Figura 15-15(*c*). Logo, x', y' e z' são representados, respectivamente, pelos pontos na metade inferior, metade direita e duas quartas partes intermediárias do mapa.

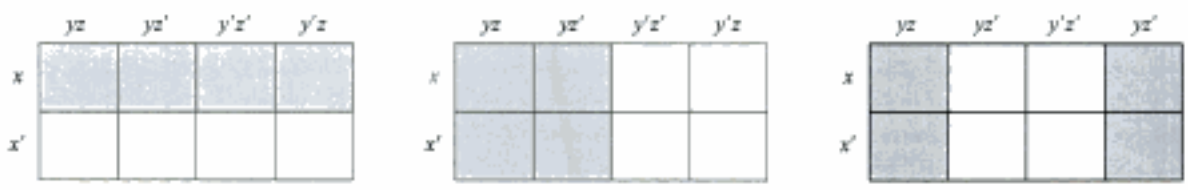


Fig. 15-15

Designamos por *retângulo básico*, no mapa de Karnaugh de três variáveis, um quadrado, dois quadrados adjacentes ou quatro quadrados que formam um retângulo de 1×4 ou 2×2 quadrados. Os retângulos básicos correspondem aos produtos fundamentais de três, dois e um literais, respectivamente. Além do mais, o produto fundamental representado por um retângulo básico é exatamente o produto dos literais que aparecem em cada quadrado do retângulo.

Suponha que uma expressão completa em soma de produtos $E = E(x, y, z)$ é representada no mapa de Karnaugh pela marcação dos quadrados apropriados. Um implicante primo de E será denominado um *retângulo básico maximal* de E, i.e., um retângulo básico contido em E que não está contido em nenhum retângulo básico maior em E. Uma forma minimal em soma de produtos para E consistirá em uma *cobertura minimal* de E, isto é, um número minimal de retângulos básicos maximais de E que, juntos, incluem todos os quadrados de E.

Exemplo 15.16 Ache os implicantes primos e uma soma de produtos minimal para cada uma das seguintes expressões Booleanas em soma de produtos completa:

(*a*) $E_1 = xyz + xyz' + x'yz' + x'y'z.$

(*b*) $E_2 = xyz + xyz' + xy'z + x'yz + x'y'z.$

(*c*) $E_3 = xyz + xyz' + x'yz' + x'y'z' + x'y'z.$

Isso pode ser feito usando o mapa de Karnaugh como a seguir.

(*a*) Marque os quadrados correspondentes aos quatro termos da soma como na Figura 15-16(*a*). Observe que E_1 tem três implicantes primos (retângulos básicos maximais), que estão circundados; são xy, yz' e $x'y'z$. Os três são necessários para cobrir E_1; portanto, a soma minimal para E_1 é

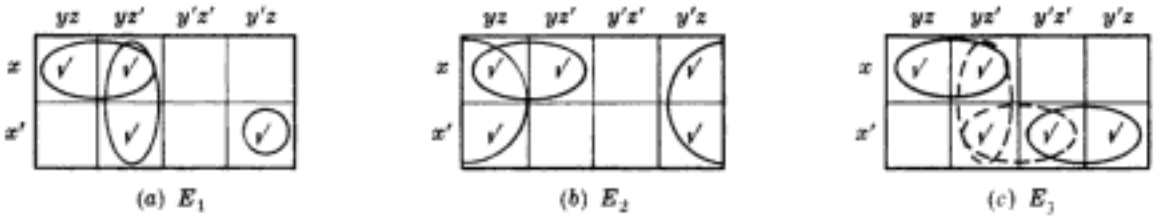
$$E_1 = xy + yz' + x'y'z$$

(*b*) Marque os quadrados correspondentes aos cinco termos da soma como na Figura 15-16(*b*). Observe que E_2 tem dois implicantes primos, que estão circundados. Um é formado pelos dois quadrados adjacentes que representam xy, e o outro é o quadrado 2×2 que representa z. Ambos são necessários para cobrir E_2, e assim a soma minimal para E_2 é

$$E_2 = xy + z$$

(*c*) Marque os quadrados correspondentes aos cinco termos da soma como na Figura 15-16(*c*). Como indicado pelos laços, E_3 tem quatro implicantes primos, xy, yz', $x'z'$ e $x'y'$. Entretanto, apenas um dentre os dois tracejados, i.e., um entre yz' ou $x'z'$, é necessário para uma cobertura minimal de E_3. Logo, E_3 tem duas somas minimais:

$$E_3 = xy + yz' + x'y' = xy + x'z' + x'y'$$



(*a*) E_1 (*b*) E_2 (*c*) E_3

Fig. 15-16

Exemplo 15.17 Projete um circuito L com três entradas, do tipo E-OU, com a tabela-verdade seguinte:

$$T = [A, B, C; L] = [00001111, 00110011, 01010101; 11001101]$$

Da tabela-verdade, podemos deduzir a forma completa em soma de produtos para L (como no Exemplo 15-10):

$$L = A'B'C' + A'B'C + AB'C' + AB'C + ABC$$

O mapa de Karnaugh associado está na Figura 15-17(*a*). Observe que L tem dois implicantes primos, B' e AC, na sua cobertura minimal; portanto, $L = B' + AC$ é uma soma minimal para L. A Figura 15-17(*b*) mostra o circuito E-OU minimal para L.

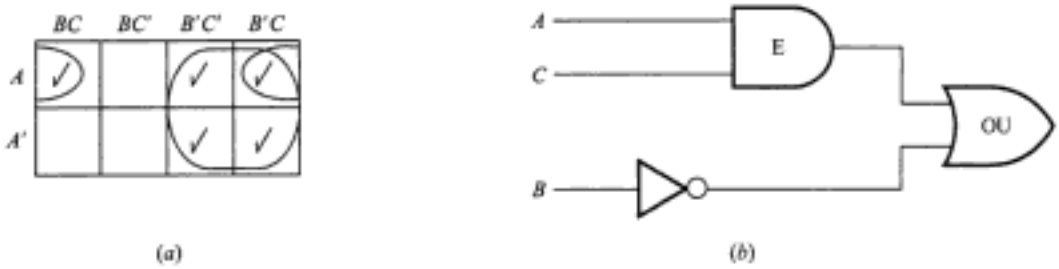


Fig. 15-17

O Caso de Quatro Variáveis

O mapa de Karnaugh correspondente a uma expressão booleana $E = E(x, y, z, t)$ com quatro variáveis x, y, z e t está mostrado na Figura 15-18. Cada um dos 16 quadrados corresponde a um dos 16 termos completos com quatro variáveis,

$$xyzt, \quad xyzt', \quad xyz't', \quad xyz't, \quad \ldots, x'yz't$$

como indicado pelos rótulos das linhas e colunas do quadrado. Observe que a linha superior e o lado esquerdo são rotulados de tal maneira que os produtos adjacentes diferem por exatamente um literal. Mais uma vez, precisamos identificar a aresta esquerda com a aresta direita (como fizemos para três variáveis), mas também precisamos identificar a aresta superior com a aresta inferior. (Essas identificações originam uma superfície em forma de rosca conhecida como *toro*, e podemos encarar nosso mapa como sendo, realmente, um toro.)

Um *retângulo básico*, no mapa de Karnaugh de quatro variáveis, é um quadrado, quatro quadrados formando um retângulo 1×4 ou 2×2 ou oito quadrados formando um retângulo 2×4. Esses retângulos correspondem aos produtos fundamentais de quatro, três, dois e um literais, respectivamente. Novamente, os retângulos básicos maximais são os implicantes primos. A técnica de minimização para uma expressão booleana $E(x, y, z, t)$ é a mesma que a anteriormente descrita.

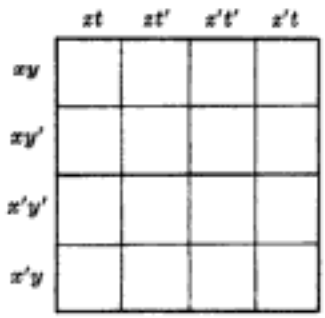


Fig. 15-18

Exemplo 15.18 Ache o produto fundamental P representado pelo retângulo básico nos mapas de Karnaugh mostrados na Figura 15-19.

Em cada caso, determine os literais que aparecem em todos os quadrados do retângulo básico; P é o produto destes literais.

(*a*) x, y e z' aparecem em ambos os quadrados; portanto, $P = xy'z'$.

(*b*) Apenas y e z aparecem nos quatro quadrados; portanto, $P = yz$.

(*c*) Apenas t aparece nos oito quadrados; portanto, $P = t$.

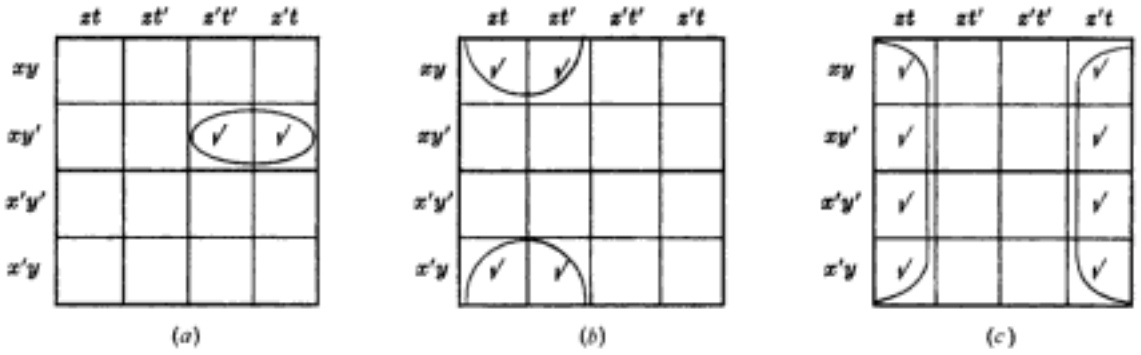


Fig. 15-19

Exemplo 15.19 Use o mapa de Karnaugh para achar uma forma minimal em soma de produtos para

$$E = xy' + xyz + x'y'z' + x'yzt'$$

Marque os quadrados que representam cada produto fundamental. Isto é, marque os quatro quadrados representando xy', os dois quadrados representando xyz, os dois quadrados representando $x'y'z'$ e o quadrado representando $x'yzt'$, como na Figura 15-20. Uma cobertura minimal do mapa consiste nos três retângulos básicos maximais identificados. Os quadrados 2×2 representam os produtos fundamentais xz e $y'z'$, e o dois quadrados adjacentes (superior e inferior) representam yzt'. Portanto,

$$E = xz + y'z' + yzt'$$

é uma soma minimal para E.

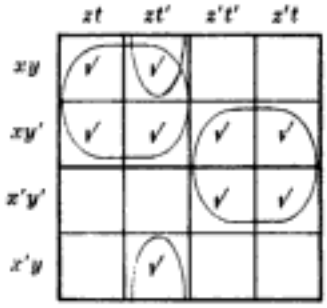


Fig. 15-20

Problemas Resolvidos

Álgebras Booleanas

15.1 Escreva a dual de cada uma das equações booleanas: (*a*) $(a * 1) * (0 + a') = 0$; (*b*) $a + a'b = a + b$.

(*a*) Para obter a equação dual, troque + e *, e troque 0 e 1. Assim,

$$(a + 0) + (1 * a') = 1$$

(*b*) Primeiramente escreva a equação usando * para obter $a + (a' * b) = a + b$. Então, o dual é $a * (a' + b) = a * b$ que pode ser escrito como

$$a(a' + b) = ab$$

15.2 Lembre (Capítulo 14) que o conjunto $\mathbf{D}_m$ de divisores de m é um reticulado distributivo limitado com $a + b = a \vee b = \text{mmc}(a, b)$ e $a * b + a \wedge b = \text{mdc}(a, b)$. (*a*) Mostre que $\mathbf{D}_m$ é uma álgebra booleana se m é um produto de primos distintos. (*b*) Ache os átomos de $\mathbf{D}_m$.

(*a*) Basta mostrar que $\mathbf{D}_m$ é complementado. Seja x em $\mathbf{D}_m$ e seja $x' = m/x$. Como m é um produto de primos distintos, x e x' têm divisores primos diferentes. Portanto, $x * x' = \text{mdc}(x, x') = 1$, e $x + x' = \text{mmc}(x, x') = m$. Lembre que 1 é o elemento zero (limite inferior) de $\mathbf{D}_m$ e que m é o elemento identidade (limite superior) de $\mathbf{D}_m$. Logo, x' é um complemento de x e, portanto, $\mathbf{D}_m$ é uma álgebra booleana.

(*b*) Os átomos de $\mathbf{D}_m$ são os divisores primos de m.

15.3 Considere a álgebra booleana $\mathbf{D}_{210}$.

(*a*) Liste seus elementos e desenhe seu diagrama.

(*b*) Ache o conjunto A de átomos.

(*c*) Ache duas subálgebras com oito elementos.

(*d*) $X = \{1, 2, 6, 210\}$ é um sub-reticulado de $\mathbf{D}_{210}$? Uma subálgebra?

(*e*) $Y = \{1, 2, 3, 6\}$ é um sub-reticulado de $\mathbf{D}_{210}$? Uma subálgebra?

(*a*) Os divisores de 210 são 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105 e 210. Os diagramas de $\mathbf{D}_{210}$ aparecem na Figura 15-21.

(*b*) $A = \{2, 3, 5, 7\}$, o conjunto de divisores primos de 210.

(*c*) $B = \{1, 2, 3, 35, 6, 70, 105, 210\}$ e $C = \{1, 5, 6, 7, 30, 35, 42, 210\}$ são subálgebras de 210.

(*d*) X é um sub-reticulado, já que é ordenado linearmente. Entretanto, X não é uma subálgebra, pois 35 é o complemento de 2 em $\mathbf{D}_{210}$ e 35 não pertence a X. (Na verdade, nenhuma álgebra booleana com mais de dois elementos é ordenada linearmente.)

(*e*) Y é um sub-reticulado de $\mathbf{D}_{210}$ pois é fechado sob + e *. Entretanto, Y não é uma subálgebra de $\mathbf{D}_{210}$ pois não é fechado sob complementos em $\mathbf{D}_{210}$; por exemplo, $35 = 2'$ não pertence a Y. (Notamos que Y é, em si, uma álgebra booleana; de fato, $Y = \mathbf{D}_6$)

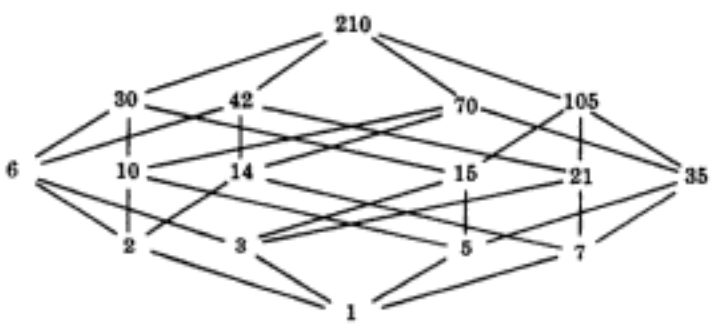


Fig. 15-21

15.4 Ache o número de subálgebras de $\mathbf{D}_{210}$.

Uma subálgebra de $\mathbf{D}_{210}$ deve conter dois, quatro, oito ou dezesseis elementos.

(i) Só pode existir uma subálgebra com dois elementos que consista no limite superior 210 e no limite inferior 1, i.e., $\{1, 210\}$.

(ii) Como $\mathbf{D}_{210}$ contém dezesseis elementos, a única subálgebra de $\mathbf{D}_{210}$ é ela mesma.

(iii) Qualquer subálgebra de quatro elementos é da forma $\{1, x, x', 210\}$, i.e., consiste nos limites inferior e superior, em um outro elemento que não é limite e seu complemento. Existem quatorze elementos que não são limite em $\mathbf{D}_{210}$ e, portanto, existem $14/2 = 7$ pares $\{x, x'\}$. Logo, $\mathbf{D}_{210}$ tem sete subálgebras com quatro elementos.

(iv) Qualquer subálgebra S com oito elementos conterá três átomos s_1, s_2, s_3. Podemos escolher s_1 e s_2 como sendo quaisquer dois dos quatro átomos de $\mathbf{D}_{210}$ e, neste caso, s_3 será o produto dos dois outros átomos, por exemplo, podemos fazer $s_1 = 2$, $s_2 = 3$, $s_3 = 5 \cdot 7 = 35$ (que determina a subálgebra B acima), ou podemos tomar $s_1 = 5$, $s_2 = 7$, $s_3 = 2 \cdot 3 = 6$ (que determina a subálgebra C acima). Existem $\binom{4}{2} = 6$ maneiras de escolher s_1 e s_2 dentre os quatro átomos de $\mathbf{D}_{210}$ e, portanto, $\mathbf{D}_{210}$ tem seis subálgebras com oito elementos.

Conseqüentemente, $\mathbf{D}_{210}$ tem $1 + 1 + 7 + 6 = 15$ subálgebras.

15.5 Prove o teorema 15.2: sejam a, b e c elementos quaisquer em uma álgebra booleana B.

(i) Leis de idempotência:

$(5a)$ $a + a = a$ $(5b)$ $a * a = a$

(ii) Leis de limitação:

$(6a)$ $a + 1 = 1$ $(6b)$ $a * 0 = 0$

(iii) Leis de absorção:

$(7a)$ $a + (a * b) = a$ $(7b)$ $a * (a + b) = a$

(iv) Leis da associatividade

$(8a)$ $(a + b) + c = a + (b + c)$ $(8b)$ $(a * b) * c = a * (b * c)$

$(5b)$ $a = a * 1 = a * (a + a') = (a * a) + (a * a') = (a * a) + 0 = a * a$

$(5a)$ Resulta de $(5b)$ e dualidade.

$(6b)$ $a * 0 = (a * 0) + 0 = (a * 0) + (a * a') = a * (0 + a') = a * (a' + 0) = a * a' = 0$

$(6a)$ Resulta de $(6b)$ e dualidade.

$(7b)$ $a * (a + b) = (a + 0) * (a + b) = a + (0 * b) = a + (b * 0) = a + 0 = a$

$(7a)$ Resulta de $(7b)$ e dualidade.

$(8b)$ Seja $L = (a * b) * c$ e $R = a * (b * c)$. Precisamos mostrar que $L = R$. Provamos primeiramente que $a + L = a + R$. Usando as leis de absorção nos dois últimos passos,

$$a + L = a + ((a * b) * c) = (a + (a * b)) * (a + c) = a * (a + c) = a$$

Usando ainda a lei de absorção no último passo,

$$a + R = a + (a * (b * c)) = (a + a) * (a + (b * c)) = a * (a + (b * c)) = a$$

Logo, $a + L = a + R$. Provaremos agora que $a' + L = a' + R$. Temos

$$\begin{aligned} a' + L &= a' + ((a * b) * c) = (a' + (a * b)) * (a' + c) \\ &= ((a' + a) * (a' + b)) * (a' + c) = (1 * (a' + b)) * (a' + c) \\ &= (a' + b) * (a' + c) = a' + (b * c) \end{aligned}$$

Além disso,

$$\begin{aligned} a' + R &= a' + (a * (b * c)) = (a' + a) * (a' + (b * c)) \\ &= 1 * (a' + (b * c)) = a' + (b * c) \end{aligned}$$

Logo, $a' + L = a' + R$. Conseqüentemente,

$$\begin{aligned} L &= 0 + L = (a * a') + L = (a + L) * (a' + L) = (a + R) * (a' + R) \\ &= (a * a') + R = 0 + R = R \end{aligned}$$

$(8a)$ Resulta de $(8b)$ e dualidade.

15.6 Prove o Teorema 15.3: seja a um elemento qualquer de uma álgebra booleana B.

(i) (Unicidade do complemento) se $a + x = 1$ e $a * x = 0$, então $x = a'$.

(ii) (Lei de involução) $(a')' = a$.

(iii) $(9a)$ $0' = 1$. $(9b)$ $1' = 0$.

(i) Temos

$$a' = a' + 0 = a' + (a * x) = (a' + a) * (a' + x) = 1 * (a' + x) = a' + x$$

Além disso,

$$x = x + 0 = x + (a * a') = (x + a) * (x + a') = 1 * (x + a') = x + a'$$

Logo, $x = x + a' = a' + x = a'$.

(ii) Pela definição de complemento, $a + a' = 1$ e $a * a' = 0$. Pela comutatividade, $a' + a = 1$ e $a' * a = 0$. Pela unicidade do complemento, a é o complemento de a', isto é, $a = (a')'$.

(iii) Pela lei da limitação (6a), $0 + 1 = 1$, e pelo axioma de identidade (3b), $0 * 1 = 0$. Pela unicidade do complemento, 1 é o complemento de 0, isto é, $1 = 0'$. Por dualidade, $0 = 1'$.

15.7 Prove o Teorema 15.4: (Leis de DeMorgan) (10a) $(a + b)' = a' * b'$. (10b) $(a * b)' = a' + b'$.

(10a) Precisamos mostrar que $(a + b) + (a' * b') = 1$ e $(a + b) * (a' * b') = 0$. Neste caso, pela unicidade do complemento, $a' * b' = (a + b')$. Temos

$$\begin{aligned}(a + b) + (a' * b') &= b + a + (a' * b') = b + (a + a') * (a + b') \\ &= b + 1 * (a + b') = b + a + b' = b + b' + a = 1 + a = 1\end{aligned}$$

Além disso,

$$\begin{aligned}(a + b) * (a' * b') &= ((a + b) * a') * b' \\ &= ((a * a') + (b * a')) * b' = (0 + (b * a')) * b' \\ &= (b * a') * b' = (b * b') * a' = 0 * a' = 0\end{aligned}$$

Logo, $a' * b' = (a + b)'$.

(10b) Princípio de dualidade (Teorema 15.1).

15.8 Prove o Teorema 15.5: Em uma álgebra booleana, são equivalentes:

(*1*) $a + b = b$, (*2*) $a * b = a$, (*3*) $a' + b = 1$, (*4*) $a * b' = 0$.

Pelo Teorema 14.4, (*1*) e (*2*) são equivalentes. Mostraremos que (*1*) e (*3*) são equivalentes. Suponha que (*1*) vale. Então,

$$a' + b = a' + (a + b) = (a' + a) + b = 1 + b = 1$$

Agora suponha que (*3*) vale. Logo,

$$a + b = 1 * (a + b) = (a' + b) * (a + b) = (a' * a) + b = 0 + b = b$$

Logo, (*1*) e (*3*) são equivalentes.

A seguir, mostramos que (*3*) e (*4*) são equivalentes. Suponha que (*3*) vale. Pela lei de DeMorgan e involução,

$$0 = 1' = (a' + b')' = a'' * b' = a * b'$$

Conversamente, se (*4*) vale

$$1 = 0' = (a * b')' = a' + b'' = a' + b$$

Portanto, (*3*) e (*4*) são equivalentes. Conseqüentemente, as quatro são equivalentes.

15.9 Prove o Teorema 15.6: A função $f: B \to P(A)$ é um isomorfismo, onde B é uma álgebra booleana, $P(A)$ é o conjunto das partes do conjunto de átomos A e

$$f(x) = \{a_1, a_2, \ldots, a_n\}$$

onde $x = a_1 + \cdots + a_n$ é a representação única de a como uma soma de átomos.

Lembre (Capítulo 14) de que se os as são átomos, então $a_i^2 = a_i$ mas $a_i a_j = 0$ para $a_i \neq a_j$. Suponha que x, y pertence a B, e suponha que

$$\begin{aligned}x &= a_1 + \cdots + a_r + b_1 + \cdots + b_s \\ y &= b_1 + \cdots + b_s + c_1 + \cdots + c_t\end{aligned}$$

onde

$$A = \{a_1, \ldots, a_r, b_1, \ldots, b_s, c_1, \ldots, c_t, d_1, \ldots, d_k\}$$

é o conjunto de átomos de B. Então,

$$\begin{aligned}x + y &= a_1 + \cdots + a_r + b_1 + \cdots + b_s + c_1 + \cdots + c_t \\ xy &= b_1 + \cdots + b_s\end{aligned}$$

Portanto,

$$\begin{aligned} f(x+y) &= \{a_1,\ldots,a_r,b_1,\ldots,b_s,c_1,\ldots,c_t\} \\ &= \{a_1,\ldots,a_r,b_1,\ldots,b_s\} \cup \{b_1,\ldots,b_s,c_1,\ldots,c_t\} \\ &= f(x) \cup f(y) \\ f(xy) &= \{b_1,\ldots,b_s\} \\ &= \{a_1,\ldots,a_r,b_1,\ldots,b_s\} \cap \{b_1,\ldots,b_s,c_1,\ldots,c_t\} \\ &= f(x) \cap f(y) \end{aligned}$$

Seja

$y = c_1 + \cdots + c_t + d_1 + \cdots + d_k$. Então, $x + y = 1$ e $xy = 0$ e, portanto, $y = x'$.

Logo,

$$f(x') = \{c_1,\ldots,c_t,d_1,\ldots,d_k\} = \{a_1,\ldots,a_r,b_1,\ldots,b_s\}^c = (f(x))^c$$

Como a representação é única, f é injetora e sobrejetora. Portanto, f é um isomorfismo de álgebras booleanas.

Expressões Booleanas

15.10 Reduza os seguintes produtos a 0 ou a um produto fundamental:

(*a*) $xyx'z$; (*b*) $xyzy$; (*c*) $xyz'yx$; (*d*) $xyz'yx'z'$.

Use a lei da comutatividade $x * y = y * x$, a lei dos complementos $x * x' = 0$ e a lei de idempotência $x * x = x$:

(*a*) $zyx'z = xx'yz = 0yz = 0$

(*b*) $xyzy = xyyz = xyz$.

(*c*) $xyz'yx = xxyyz' = xyz'$.

(*d*) $xyz'yx'z' = xx'yyz'z' = 0yz' = 0$.

15.11 Expresse cada expressão booleana $E(x, y, z)$ como soma de produtos e depois na sua forma completa em soma de produtos: (*a*) $E = x(xy' + x'y + y'z)$; (*b*) $E = z(x' + y) + y'$.

Primeiramente use o Algoritmo 15.8A para expressar E como uma soma de produtos, e depois o Algoritmo 15.8B para expressar E como uma soma de produtos completa.

(*a*) Temos primeiramente $E = xxy' + xx'y + xy'z = xy' + xy'z$. Então,

$$E = xy'(z + z') + xy'z = xy'z + xy'z' + xy'z = xy'z + xy'z'$$

(*b*) Temos primeiramente

$$E = z(x' + y) + y' = x'z + yz + y'$$

Então,

$$\begin{aligned} E &= x'z + yz + y' = x'z(y + y') + yz(x + x') + y'(x + x')(z + z') \\ &= x'yz + x'y'z + xyz + x'yz + xy'z + xy'z' + x'y'z + x'y'z \\ &= xyz + xy'z + xy'z' + x'yz + x'y'z + x'y'z' \end{aligned}$$

15.12 Expresse $E(x, y, z) = (x' + y)' + x'y$ na sua forma completa em soma de produtos.

Temos $E = (x' + y)' + x'y = xy' + x'y$, que seria a forma completa em soma de produtos de E se E fosse uma expressão booleana em x e y. Entretanto, está especificado que E é uma expressão booleana nas variáveis x, y e z. Portanto,

$$E = xy' + x'y = xy'(z + z') + x'y(z + z') = xy'z + xy'z' + x'yz + x'yz'$$

é a forma completa em soma de produtos de E.

15.13 Expresse cada expressão booleana $E(x, y, z)$ como soma de produtos e depois na sua forma completa em soma de produtos: (*a*) $E = y(x + yz)'$; (*b*) $E = x(xy + y' + x'y)$.

(*a*) $E = y(x'(yz)') = yx'(y' + z') = yx'y' + x'yz' = x'yz'$

que já está na forma completa em soma de produtos.

(*b*) Primeiramente temos $E = xxy + xy' + xx'y = xy + xy'$. Depois,

$$E = xy(z + z') + xy'(z + z') = xyz + xyz' + xy'z + xy'z'$$

15.14 Expresse cada expressão $E(A, B, C)$ envolvendo os conjuntos A, B e C como união de interseções.

(*a*) $E = (A \cup B)^c \cap (C^c \cup B)$; (*b*) $E = (B \cap C)^c \cap (A^c \cap C)^c$

Use notação booleana ' para complemento, + para união e * (ou justaposição) para interseção, e assim expresse E como uma soma de produtos (união de interseções).

(*a*) $E = (A + B)'(C' + B) = A'B'(C' + B) = A'B'C' + A'B'B = A'B'C'$ ou $E = A^c \cap B^c \cap C^c$.

(*b*) $E = (BC)'(A' + C)' = (B' + C')(AC') = AB'C' + AC'$ ou $E = (A \cap B^c \cap C^c) \cup (A \cap C^c)$.

15.15 Seja $E = xy' + xyz' + x'yz'$. Prove que: (*a*) $xz' + E = E$; (*b*) $x + E \neq E$; (*c*) $z' + E \neq E$.

Como a forma completa em soma de produtos é única, $A + E = E$, onde $A \neq 0$, se e somente se os termos de soma na forma completa em soma de produtos de A estão entre os termos de soma na forma completa em soma de produtos de E. Portanto, ache primeiramente a forma completa em soma de produtos de E.

$$E = xy'(z + z') + xyz' + x'yz' = xy'z + xy'z' + xyz' + x'yz'$$

(*a*) Expresse xz' na forma completa em soma de produtos:

$$xz' = xz'(y + y') = xyz' + xy'z'$$

Como os termos da soma de xz' estão entre os termos da soma de E, temos $xz' + E = E$.

(*b*) Expresse x na forma completa em soma de produtos:

$$x = x(y + y')(z + z') = xyz + xyz' + xy'z + xy'z'$$

O termo xyz da soma de x não está entre os termos da soma de E; portanto, $x + E \neq E$.

(*c*) Expresse z' na forma completa em soma de produtos:

$$z' = z'(x + x')(y + y') = xyz' + xy'z' + x'yz' + x'y'z'$$

O termo $x'y'z'$ da soma de z' não está entre os termos da soma de E; portanto, $z' + E \neq E$.

Expressões Booleanas Minimais e Implicantes Primos

15.16 Para uma expressão booleana qualquer E na forma de soma de produtos, denote por E_L o número de literais em E (contando a multiplicidade) e por E_S o número de termos na soma de E. Ache E_L e E_S para cada uma das expressões seguintes:

(*a*) $E = xy'z + x'z' + yz' + x$. (*c*) $E = xyt' + x'y'zt + xz't$.

(*b*) $E = x'y'z + xyz + y + yz' + x'z$. (*d*) $E = (xy' + z)' + xy'$.

Simplesmente some o número de literais e o número de termos da soma em cada expressão:

(*a*) $E_L = 3 + 2 + 2 + 1 - 8$, $E_S = 4$.

(*b*) $E_L = 3 + 3 + 1 + 2 + 2 = 11$, $E_S = 5$.

(*c*) $E_L = 3 + 4 + 3 = 10$, $E_S = 3$.

(*d*) Como E não é escrito como uma soma de produtos, E_L e E_S não são definidos.

15.17 Sabendo que E e F são expressões booleanas equivalentes na forma de soma de produtos, defina: (*a*) E é mais simples do que F; (*b*) E é minimal.

(*a*) E é mais simples do que F se $E_L < F_L$ e $E_S \leq F_S$, ou se $E_L \leq F_L$ e $E_S < F_S$.

(*b*) E é minimal se não existe expressão equivalente em soma de produtos mais simples do que E.

15.18 Ache o *consensus* Q dos produtos fundamentais P_1 e P_2 onde:

(*a*) $P_1 = xy'z'$, $P_2 = xyt$. (*c*) $P_1 = xy'z'$, $P_2 = x'y'zt$.

(*b*) $P_1 = xyz't$, $P_2 = xzt$. (*d*) $P_1 = xyz'$, $P_2 = xz't$.

O *consensus* Q de P_1 e P_2 existe se existir exatamente uma variável, digamos, x_k, que é complementada em um dentre P_1 e P_2 e não complementada no outro. Então, Q é o produto (sem repetição) de literais em P_1 e P_2 depois que x_k e x_k' foram deletados.

(*a*) Delete y e y' e depois multiplique os literais de P_1 e P_2 (sem repetição) para obter $Q = xz't$.

(*b*) Deletando z' e z, obtém-se $Q = xyt$.

(*c*) Eles não têm *consensus*, já que as variáveis x e z aparecem complementadas em um dos produtos e não complementada no outro.

(*d*) Eles não têm *consensus*, já que nenhuma variável aparece complementada em um dos produtos e não complementada no outro.

15.19 Prove o Lema 15.10: suponha que Q é o *consensus* de P_1 e P_2. Então, $P_1 + P_2 + Q = P_1 + P_2$.

Como os literais comutam, podemos assumir, sem perda de generalidade, que

$$P_1 = a_1a_2 \cdots a_r t, \qquad P_2 = b_1b_2 \cdots b_s t', \qquad Q = a_1a_2 \cdots a_r b_1b_2 \cdots b_s$$

Porém, $Q = Q(t + t') = Qt + Qt'$. Como Qt contém P_1, $P_1 + Qt = P_1$; e porque Qt' contém P_2, $P_2 + Qt' = P_2$. Portanto,

$$P_1 + P_2 + Q = P_1 + P_2 + Qt + Qt' = (P_1 + Qt) + (P_2 + Qt') = P_1 + P_2$$

15.20 Seja $E = xy' + xyz' + x'yz'$. Ache: (*a*) os implicantes primos de E; (*b*) uma soma minimal para E.

(*a*) Use o Algoritmo 15.9A (método do *consensus*) como a seguir:

$$\begin{aligned} E &= xy' + xyz' + x'yz' + xz' && (\textit{consensus de } xy' \text{ e } xyz') \\ &= xy' + x'yz' + xz' && (xyz' \text{ inclui } xz') \\ &= xy' + x'yz' + xz' + yz' && (\textit{consensus de } x'yz' \text{ e } xz') \\ &= xy' + xz' + yz' && (x'yz' \text{ inclui } yz') \end{aligned}$$

Nenhum dos passos do método de *consensus* pode ser aplicado agora. Portanto, xy', xz' e yz' são os implicantes primos de E.

(*b*) Aplique o Algoritmo 15.9B. Escreva cada implicante primo de E em forma de uma soma de produtos completa obtendo:

$$\begin{aligned} xy' &= xy'(z + z') = xy'z + xy'z' \\ xz' &= xz'(y + y') = xyz' + xy'z' \\ yz' &= yz'(x + x') = xyz' + x'yz' \end{aligned}$$

Apenas os termos de soma xyz' e $xy'z'$ de xz' aparecem entre os outros termos de soma e, portanto, xz' pode ser considerado supérfluo e eliminado. Logo, $E = xy' + yz'$ é uma soma minimal de E.

15.21 Seja $E = xy' + y't + x'yz' + xy'zt'$. Ache: (*a*) os implicantes primos de E; (*b*) uma soma minimal para E.

(*a*) Use o Algoritmo 15.9A (Método do *consensus*) como a seguir:

$$
\begin{aligned}
E &= xy + y't + x'yz' + xy'zt' + xzt' && (\textit{consensus}\ \text{de}\ xy\ \text{e}\ xy'zt') \\
&= xy + y't + x'yz' + xzt' && (xy'zt'\ \text{inclui}\ xzt') \\
&= xy + y't + x'yz' + xzt' + yz' && (\textit{consensus}\ \text{de}\ xy\ \text{e}\ x'yz') \\
&= xy + y't + xzt' + yz' && (x'yz'\ \text{inclui}\ yz') \\
&= xy + y't + xzt' + yz' + xt && (\textit{consensus}\ \text{de}\ xy\ \text{e}\ y't) \\
&= xy + y't + xzt' + yz' + xt + xz && (\textit{consensus}\ \text{de}\ xzt'\ \text{e}\ xt) \\
&= xy + y't + yz' + xt + xz && (xzt'\ \text{inclui}\ xz) \\
&= xy + y't + yz' + xt + xz + z' && (\textit{consensus}\ \text{de}\ y't\ \text{e}\ yz')
\end{aligned}
$$

Nenhum dos passos do método de *consensus* pode ser aplicado agora. Portanto, os implicantes primos de E são yz', xt, xz e $z't$.

(*b*) Aplique o Algoritmo 15.9B. Escreva cada implicante primo em forma de uma soma de produtos completa e depois delete, um por um, os que são supérfluos, i.e., aqueles cujos termos da soma aparecem entre outros termos de soma. Este procedimento produz no final

$$E = y't + xz + yz'$$

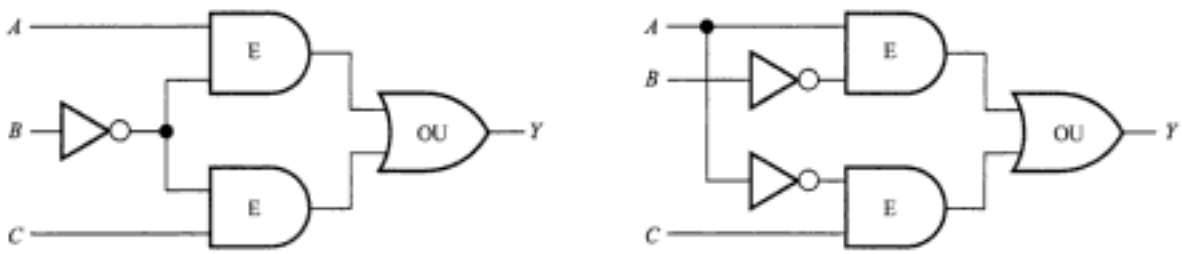
como uma soma minimal de E.

Portas Lógicas

15.22 Expresse a saída Y como expressão booleana em função das entradas A, B, C para o circuito lógico em: (*a*) Figura 15.22(*a*); (*b*) Figura 15.22(*b*).

(*a*) As entradas para a primeira porta OU são A e B', e para a segunda porta E são B' e C. Portanto, $Y = AB' + B'C$.

(*b*) As entradas para a primeira porta E são A e B', e para a segunda porta E são A' e C. Logo, $Y = AB' + A'C$.



(*a*) (*b*)

Fig. 15-22

15.23 Expresse a saída Y como expressão booleana em função das entradas A, B, C para o circuito lógico da Figura 15-23.

A saída da primeira porta E é $A'BC$, da segunda porta E é $AB'C'$ e da última porta E é AB'. Logo,

$$Y = A'BC + AB'C' + AB'$$

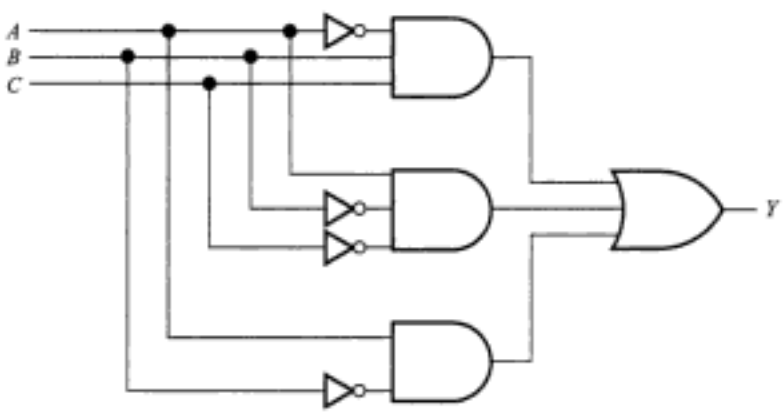


Fig. 15-23

15.24 Expresse a saída Y como expressão booleana em função das entradas A, B, C para o circuito lógico em: (*a*) Figura 15.24(*a*); (*b*) Figura 15.24(*b*).

(*a*) A saída da porta E é BC e, assim, as entradas para as portas NOU são A e BC. Logo, $(A + BC)'$ é a saída da porta NOU. Portanto, as entradas para a porta OU são $(A + BC)'$ e B; portanto, $Y = (A + BC)' + B$.

(*b*) A saída da porta NE é $(A'B)'$ e a saída da porta NOU é $(A + C)'$. Logo, $Y = (A'B)' + (A + C)'$.

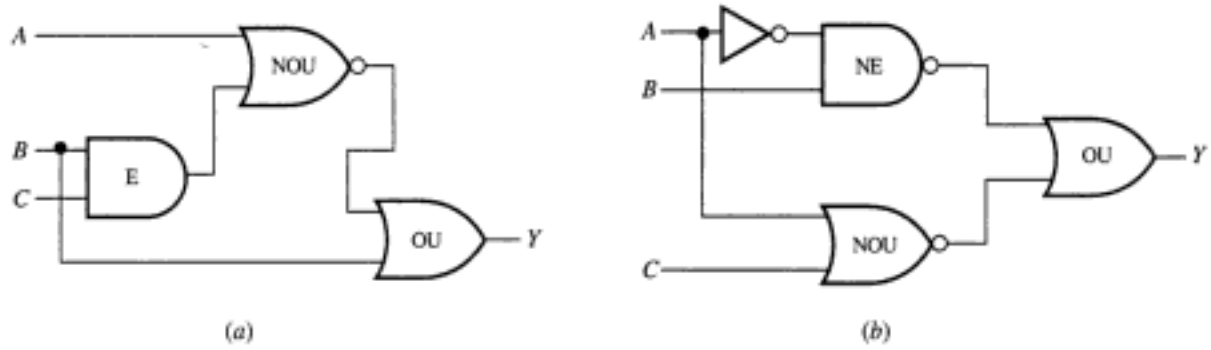


Fig. 15-24

15.25 Expresse a saída Y como expressão booleana em função das entradas A e B para o circuito lógico da Figura 15-25.

Aqui, um pequeno círculo no circuito significa complemento. Logo, as saídas das três portas da esquerda são AB', $(A + B)'$ e $(A'B)'$. Portanto,

$$Y = AB' + (A + B)' + (A'B)'$$

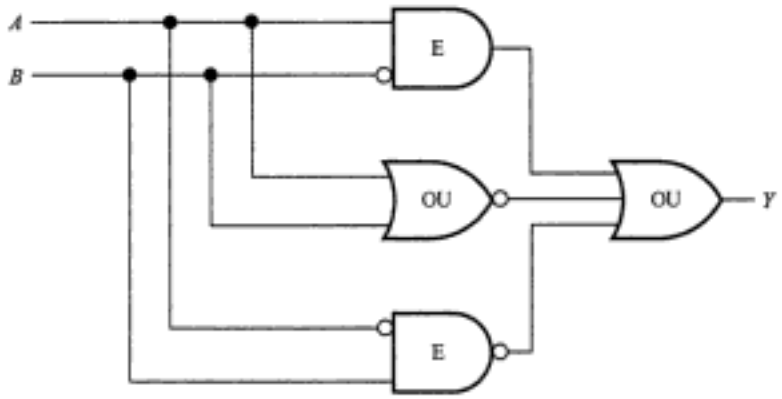


Fig. 15-25

15.26 Desenhe o circuito lógico L com entradas A, B e C e saída Y correspondente a cada expressão booleana:

(*a*) $Y = ABC + A'C' + B'C'$; (*b*) $Y = AB'C + ABC' + AB'C'$.

Estas expressões estão em forma de soma de produtos. Logo, L será um circuito E-OU que tem uma porta E para cada produto e uma porta OU para a soma. Os circuitos em questão aparecem na Figura 15-26(*a*) e 15-26(*b*).

Hidden page

15.30 Considere um circuito lógico L com $n = 5$ entradas A, B, C, D, E, ou, equivalentemente, considere uma expressão booleana E com cinco variáveis x_1, x_2, x_3, x_4, x_5.

(*a*) Ache as seqüências especiais para as variáveis (entradas).

(*b*) De quantas maneiras distintas pode-se atribuir um *bit* (0 ou 1) a cada uma das $n = 5$ variáveis?

(*c*) Qual a propriedade principal das seqüências especiais?

(*a*) Todas as seqüências têm comprimento $2^n = 2^5 = 32$. Elas consistirão em blocos alternados de 0s e 1s onde o comprimento dos blocos são $2^{n-1} = 2^4 = 16$ para x_1, $2^{n-2} = 2^3 = 8$ para $x_2, \ldots, 2^{n-5} = 2^0 = 1$ para x_5. Logo,

$$x_1 = 00000000000000001111111111111111$$
$$x_2 = 00000000111111110000000011111111$$
$$x_3 = 00001111000011110000111100001111$$
$$x_4 = 00110011001100110011001100110011$$
$$x_5 = 01010101010101010101010101010101$$

(*b*) Existem duas maneiras, 0 ou 1, de atribuir *bits* a cada variável e, portanto, existem $2^n = 2^5 = 32$ maneiras de atribuir um *bit* a cada uma das $n = 5$ variáveis.

(*c*) As 32 posições nas seqüências especiais dão todas as 32 combinações de *bits* possíveis para as cinco variáveis.

15.31 Ache a tabela-verdade para $T = T(E)$ para a expressão booleana $E = E(x, y, z)$ onde

(*a*) $E = xz + x'y$; (*b*) $E = xy'z + xy + z'$.

As seqüências especiais para as variáveis (x, y, z) e seus complementos são:

$$x = 00001111, \quad y = 00110011, \quad z = 01010101$$
$$x' = 11110000, \quad y' = 11001100, \quad z' = 10101010$$

(*a*) Neste caso, $xz = 00000101$ e $x'y = 00110000$. Logo, $E = xz + x'y = 00110101$. Logo,

$$T(00001111,\ 00110011,\ 01010101) = 00110101$$

ou, simplesmente, $T(E) = 00110101$ onde assumimos que a entrada consiste nas seqüências especiais.

(*b*) Aqui, $xy'z = 00000100$, $xy = 00000011$ e $z' = 01010101$. Então, $E = xy'z + xy + z' = 01010111$. Logo,

$$T(00001111,\ 00110011,\ 01010101) = 01010111$$

15.32 Ache a tabela-verdade para $T = T(E)$ para a expressão booleana $E = E(x, y, z)$ onde

(*a*) $E = xyz' + x'yz$; (*b*) $E = xyz + xy'z + x'y'z$.

Aqui E é uma soma de produtos completa que é a soma de termos completos. O Exemplo 15.13 mostra as tabelas-verdade para os termos completos (usando as seqüências especiais). Cada termo completo contém um único 1 na sua tabela-verdade; portanto, a tabela-verdade de E terá 1s na mesma posição que os termos completos em E. Logo,

(*a*) $T(E) = 00001010$; (*b*) $T(E) = 01000101$

15.33 Ache a tabela-verdade para $T = T(E)$ para a expressão booleana

$$E = E(x,\ y,\ z) = (x'y)'yz' + x'(yz + z')$$

Primeiramente expresse E como uma soma de produtos:

$$E = (x + y')yz' + x'yz + x'z' = xyz' + y'yz' + x'yz + x'z'$$
$$= xyz' + x'yz + x'z'$$

Agora expresse E como uma soma de produtos completa:

$$E = xyz' + x'yz + x'z'(y + y')$$
$$= xyz' + x'yz + x'yz' + x'y'z'$$

Como no Problema 15.32, use as tabelas-verdade para os termos completos que aparecem no Exemplo 15.13 para obt $T(E) = 10101010$.

15.34 Ache a expressão booleana $E = E(x, y, z)$ correspondente à tabela-verdade:

(*a*) $T(E) = 01001001$; (*b*) $T(E) = 00010001$.

Cada 1 em $T(E)$ corresponde ao termo completo com o 1 na mesma posição (usando as tabelas-verdade para os te mos completos que aparecem no Exemplo 15.13). Por exemplo, o 1 na segunda posição corresponde a $x'y'z$ cuja tabel verdade tem um único 1 na segunda posição. Assim, E é a soma de termos completos. Logo:

(*a*) $E = x'y'z + x'yz + xyz'$; (*b*) $E = xy'z' + xyz$

(Admitimos mais uma vez que a entrada consiste nas seqüências especiais.)

Mapas de Karnaugh

15.35 Ache o produto fundamental P representado por cada retângulo básico no mapa de Karnaugh da Figura 15-27.

Em cada caso, determine os literais que aparecem em todos os quadrados do retângulo básico; P é, então, o prod to destes literais.

(*a*) x' e z' aparecem em ambos os quadrados; portanto, $P = x'z'$.

(*b*) x e z aparecem em ambos os quadrados; portanto, $P = xz$.

(*c*) Apenas z aparece nos quatro quadrados; portanto, $P = z$.

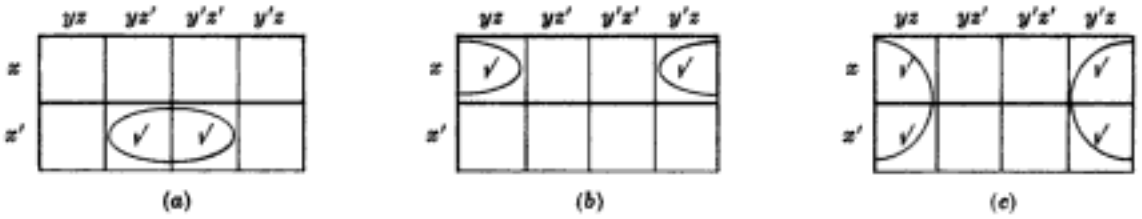


Fig. 15-27

15.36 Seja R um retângulo básico no mapa de Karnaugh para quatro variáveis x, y, z e t. Descreva o número de literais n produto fundamental P correspondente a R em termos do número de quadrados em R.

P terá um, dois, três ou quatro literais dependendo de R ter oito, quatro, dois ou um quadrado.

15.37 Ache o produto fundamental P representado por cada retângulo básico no mapa de Karnaugh da Figura 15-28.

Em cada caso, ache os literais que aparecem em todos os quadrados do retângulo básico; P é produto destes literai (O Problema 15.36 indica o número destes literais em P.)

(*a*) Existem dois quadrados em R; logo, P tem três literais. Especificamente, x', y', t' aparecem em ambos os quadrado logo, $P = x'y't'$.

(*b*) Existem quatro quadrados em R; logo, P tem dois literais. Especificamente, apenas y' e t aparecem nos quatro qu drados; logo, $P = y't$.

(*c*) Existem oito quadrados em R; logo, P tem apenas um literal. Especificamente, apenas y aparece nos oito quadrado logo, $P = y$.

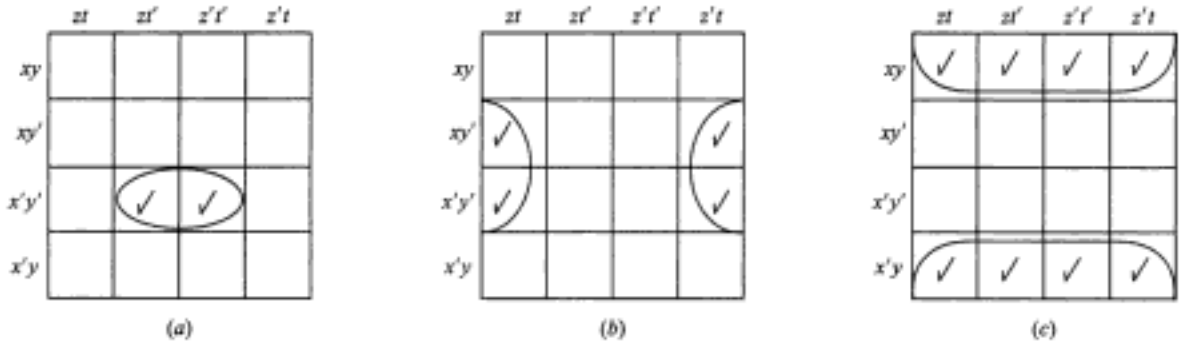


Fig. 15-28

15.38 Seja R a expressão booleana dada no mapa de Karnaugh da Figura 15-29. (*a*) Escreva E na forma de soma de produtos completa. (*b*) Ache uma forma minimal para E.

(*a*) Liste os sete produtos fundamentais marcados para obter

$$E = xyz't' + xyz't + xy'zt + xy'zt' + x'y'zt + x'y'zt' + x'yz't'$$

(*b*) Os retângulos básicos maximais 2×2 representam $y'z$, já que apenas y' e z aparecem nos quatro quadrados. O par horizontal de quadrados adjacentes representa xyz', e os quadrados adjacentes cobrindo as arestas superior e inferior representam $yz't'$. Como os três retângulos são necessários para uma cobertura minimal,

$$E = y'z + xyz' + yz't'$$

é uma soma minimal de E.

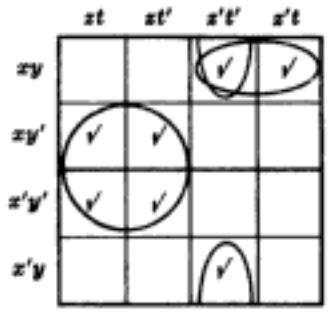


Fig. 15-29

15.39 Considere as expressões booleanas E_1 e E_2 nas variáveis x, y, z, t dadas pelo mapa de Karnaugh da Figura 15-30. Ache uma soma minimal para (*a*) E_1; (*b*) E_2.

(*a*) Apenas y' aparece em todos os oito quadrados do retângulo básico maximal 2×4, e o par de quadrados adjacentes designado representa xzt'. Como ambos os retângulos são necessários para uma cobertura minimal,

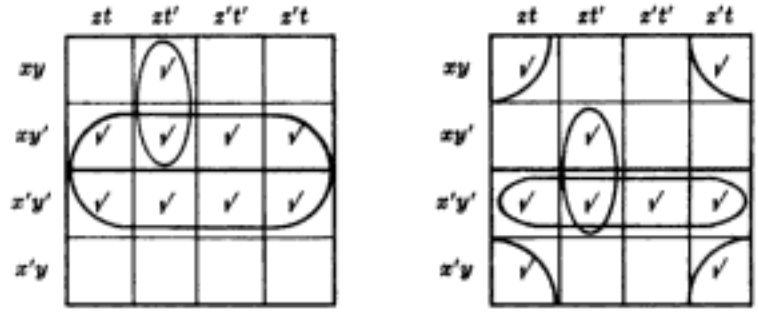
$$E_1 = y' + xzt'$$

é a soma minimal de E_1.

(*b*) Os quatro quadrados dos canto formam um retângulo básico maximal 2×2 que representa yt, já que apenas y e t aparecem nos quatro quadrados. O retângulo básico maximal 4×1 representa $x'y'$, e os dois quadrados adjacentes representam $y'zt'$. Como todos os três retângulos são necessários para uma cobertura,

$$E_2 = yt + x'y' + y'zt'$$

é a soma minimal de E_2.



(*a*) E_1 (*b*) E_2

Fig. 15-30

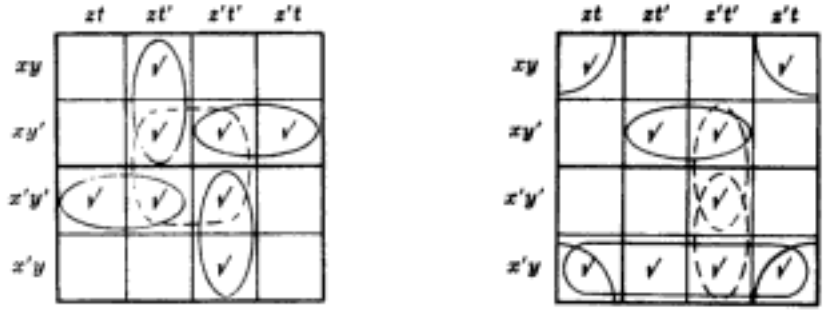
15.40 Considere as expressões booleanas E_1 e E_2 nas variáveis x, y, z, t dadas pelo mapa de Karnaugh da Figura 15-31. Ache uma soma minimal para (*a*) E_1; (*b*) E_2.

(*a*) Existem cinco implicantes primos, designados pelos quatro laços e o círculo tracejado. Entretanto, o círculo tracejado não é necessário para cobrir todos os quadrados, mas os quatro laços são. Assim, os quatro laços fornecem a soma minimal para E_1; isto é,

$$E_1 = xzt' + xy'z' + x'y'z + x'z't'$$

(*b*) Existem cinco implicantes primos, indicados pelos cinco laços, dos quais dois são tracejados. Apenas um dos laços tracejados é necessário para cobrir o quadrado $x'y'z't'$. Portanto, existem duas somas minimais para E_2, a saber:

$$E_2 = x'y + yt + xy't' + y'z't' = x'y + yt + xy't' + x'z't'$$



(*a*) E_1 (*b*) E_2

Fig. 15-31

15.41 Use o mapa de Karnaugh para achar uma soma minimal para:

(*a*) $E_1 = x'yz + x'yz't + y'zt' + xyzt' + xy'z't'$.

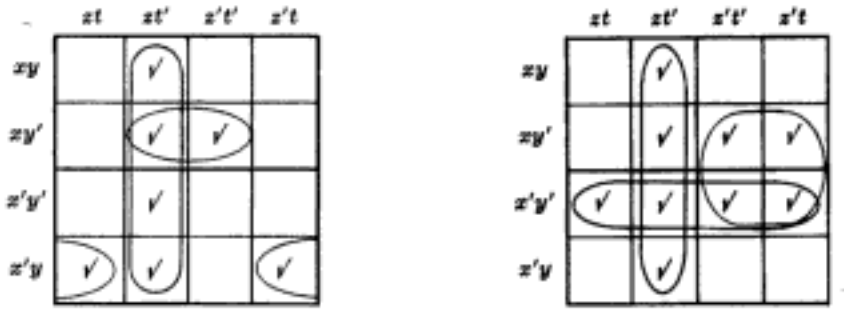
(*b*) $E_2 = y't' + y'z't + x'y'zt + yzt'$.

(*a*) Marque os dois quadrados correspondendo a cada $x'yz$ e $y'zt'$ e o quadrado que corresponde a cada $x'yz't$, $xyzt'$ e $xy'z't'$. Obtém-se assim o mapa de Karnaugh da Figura 15-32(*a*). Uma cobertura minimal consiste nos três laços indicados. Logo, uma soma minimal para E_1 é

$$E_1 = zt' + xy't' + x'yt$$

(*b*) Marque os quatro quadrados que correspondem a zt', marque os dois quadrados correspondentes a cada um dos $y'z't$ e yzt', e marque o quadrado correspondendo a $x'y'zt$. Obtém-se assim o mapa de Karnaugh da Figura 15-32(*b*). Uma cobertura minimal consiste nos três retângulos básicos maximais assinalados. Portanto, uma soma minimal para E_2 é

$$E_2 = zt' + xy't' + x'yt$$



(*a*) E_1 (*b*) E_2

Fig. 15-32

15.42 Ache uma forma minimal em soma de produtos para a expressão booleana E com as tabelas-verdade seguintes:

(*a*) $T(00001111, 00110011, 01010101) = 10100110$.

(*b*) $T(00001111, 00110011, 01010101) = 00101111$.

(*a*) A partir da tabela-verdade dada T (e das tabelas-verdade no Exemplo 15-13 para os termos completos nas variáveis x, y, z) podemos deduzir a forma completa em soma de produtos de E:

$$E = x'y'z' + x'yz' + xy'z + xyz'$$

O mapa de Karnaugh aparece na Figura 15-33(*a*). Existem três implicantes primos, como indicado pelos três laços, que formam uma cobertura minimal de E. Assim, uma forma minimal de E é

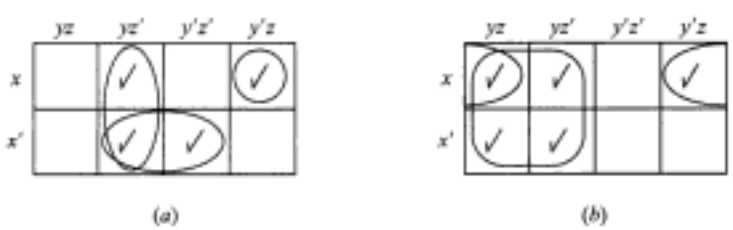
$$E = yz' + x'z' + xy'z$$

(*b*) A partir da tabela-verdade dada, podemos deduzir a forma completa em soma de produtos para E:

$$E = x'yz' + x'yz + xy'z + xyz' + xyz$$

cujo mapa de Karnaugh aparece na Figura 15-33(*b*). Existem dois implicantes primos, como indicado pelos dois laços, que formam uma cobertura minimal de E. assim, uma forma minimal de E é

$$E = xz + y$$



(*a*) (*b*)

Fig. 15-33

Problemas Complementares

Álgebras Booleanas

15.43 Escreva a expressão dual de cada uma das expressões booleanas:

(*a*) $a(a' + b) = ab$.

(*b*) $(a + 1)(a + 0) = a$.

(*c*) $(a + b)(b + c) = ac + b$.

15.44 Considere os reticulados $\mathbf{D}_m$ de divisores de m (onde $m > 1$).

(*a*) Mostre que $\mathbf{D}_m$ é uma álgebra booleana se e somente se m é *square-free*, isto é, m é um produto de primos distintos.

(*b*) Se $\mathbf{D}_m$ é uma álgebra booleana, mostre que os átomos são os divisores primos distintos de m.

15.45 Considere os seguintes reticulados: (*a*) $\mathbf{D}_{20}$; (*b*) $\mathbf{D}_{55}$; (*c*) $\mathbf{D}_{99}$; (*d*) $\mathbf{D}_{130}$. Quais deles são álgebras booleanas e quais são seus átomos?

15.46 Considere a álgebra booleana $\mathbf{D}_{110}$. (*a*) Liste seus elementos e desenhe seu diagrama. (*b*) Ache todas as suas subálgebras. (*c*) Ache o número de sub-reticulados com quatro elementos. (*d*) Ache o conjunto A de átomos de $\mathbf{D}_{110}$. (*e*) Defina um isomorfismo $f: \mathbf{D}_{110} \to P(A)$ como definido no Teorema 15.6.

15.47 Seja B uma álgebra booleana. Mostre que:

(*a*) Para todo $x \in B$, $0 \leq x \leq 1$.

(*b*) $a < b$ se e somente se $b' < a'$

15.48 Um elemento x em uma álgebra booleana é dito um *termo máximo* se o seu único sucessor é a identidade 1. Ache os termos máximos da álgebra booleana $\mathbf{D}_{210}$ representada na Figura 15-21.

15.49 Seja B uma álgebra booleana. (*a*) Mostre que os complementos dos átomos de B são os termos máximos. (*b*) Mostre que todo elemento $x \in B$ pode ser expresso de maneira única como um produto de termos máximos.

15.50 Seja B uma álgebra booleana de 16 elementos, e seja S uma subálgebra de B com oito elementos. Mostre que dois dos átomos de S devem ser átomos de B.

15.51 Seja $B = (B, +, *, ', 0, 1)$ uma álgebra booleana. Defina uma operação Δ em B (chamada diferença simétrica) por

$$x \triangle y = (x * y') + (x' * y)$$

Prove que $R = (B, \Delta, *)$ é uma anel comutativo booleano. (Veja a Seção 12.6 e o Problema 12.77.)

15.52 Seja $R = (R, \oplus, \cdot)$ um anel booleano com identidade $1 \neq 0$. Defina

$$x' = 1 \oplus x, \qquad x + y = x \oplus y \oplus x \cdot y, \qquad x * y = x \cdot y$$

Prove que $B = (B, +, *, ', 0, 1)$ é uma álgebra booleana.

Expressões Booleanas e Implicantes Primos

15.53 Reduza os produtos booleanos seguintes a 0 ou a um produto fundamental:

(*a*) $xy'zxy'$; (*b*) $xyz'sy'ts$; (*c*) $xy'xz'ty'$; (*d*) $xyz'ty't$.

15.54 Expresse cada expressão booleana $E(x, y, z)$ como uma soma de produtos, e depois na sua forma completa em soma de produtos.

(*a*) $E = x(xy' + x'y + y'z)$. (*b*) $E = (x + y'z)(y + z')$. (*c*) $E = (x' + y)' + y'z$.

15.55 Expresse cada expressão Booleana $E(x, y, z)$ como uma soma de produtos, e depois na sua forma completa em soma de produtos.

(*a*) $E = (x'y)'(x' + xyz')$. (*b*) $E = (x + y)'(xy')'$. (*c*) $E = y(x + yz)'$.

15.56 Ache o *consensus* Q dos produtos fundamentais P_1 e P_2 onde:

(*a*) $P_1 = xy'z$, $P_2 = xyt$. (*c*) $P_1 = xy'zt$, $P_2 = xyz'$.

(*b*) $P_1 = xyz't'$, $P_2 = xzt'$. (*d*) $P_1 = xy't$, $P_2 = xzt$.

15.57 Para uma expressão booleana E em soma de produtos, denote por E_L o número de literais em E (contando a multiplicidade) e por E_S o número de termos na soma de E. Ache E_L e E_S para cada uma das expressões a seguir:

(*a*) $E = xyz't + x'yt + xy'zt$. (*b*) $E = xyzt + xt' + x'y't + yt$.

15.58 Aplique o método do *consensus* (Algoritmo 15.9A) para achar os implicantes primos de cada uma das expressões booleanas:

(*a*) $E_1 = xy'z' + x'y + x'y'z' + x'yz$.

(*b*) $E_2 = xy' + x'z't + xyzt' + x'y'zt'$.

(*c*) $E_3 = xyzt + xyz't' + xz't' + x'y'z' + x'yz't$.

15.59 Ache uma forma minimal em soma de produtos para cada uma das expressões booleanas do Problema 15.58.

Portas Lógicas e Tabelas-Verdade

15.60 Expresse a saída Y como uma expressão booleana nas entradas A, B, C para o circuito lógico em: (*a*) Figura 15-34(*a*); (*b*) Figura 15-34(*b*).

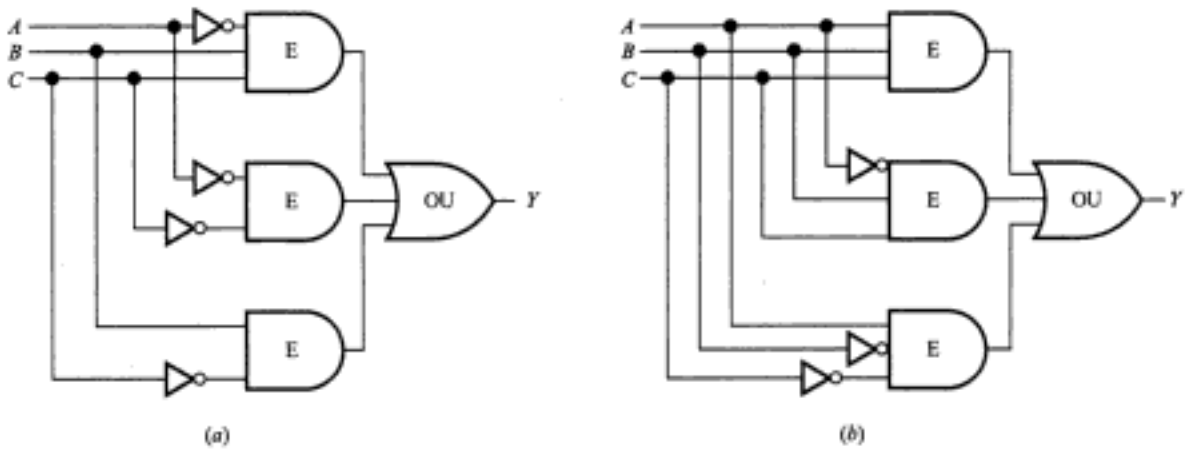


Fig. 15-34

15.61 Expresse a saída Y como uma expressão booleana nas entradas A, B, C para o circuito lógico em: (*a*) Figura 15-35(*a*); (*b*) Figura 15-35(*b*).

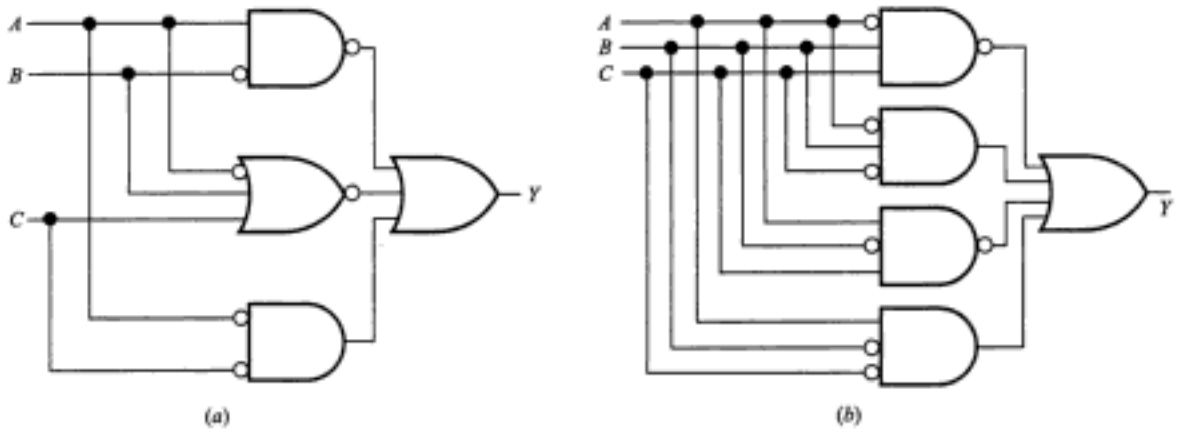


Fig. 15-35

15.62 Desenhe o circuito lógico L com entradas A, B e C e saída Y correspondente a cada uma das expressões booleanas:

(*a*) $Y = AB'C + AC' + B'C$. (*b*) $Y = A'BC + A'BC' + ABC'$

15.63 Ache a seqüência de saída Y para uma porta E com entradas A, B, C (ou, equivalentemente, para $Y = ABC$) onde:

(*a*) $A = 110001$; $B = 101101$; $C = 110011$.

(*b*) $A = 01111100$; $B = 10111010$; $C = 00111100$.

(*c*) $A = 00111110$; $B = 01111100$; $C = 11110011$.

15.64 Ache a seqüência de saída Y para uma porta OU com entradas A, B, C (ou, equivalentemente, para $Y = A + B + C$) onde:

(*a*) $A = 100011$; $B = 100101$; $C = 1000001$.

(*b*) $A = 10000001$; $B = 00100100$; $C = 00000011$.

(*c*) $A = 00111100$; $B = 11110000$; $C = 10000001$.

15.65 Ache a seqüência de saída Y para uma porta NÃO com entradas A ou, equivalentemente, para $Y = A'$ onde:

(*a*) $A = 11100111$; (*b*) $A = 10001000$; (*c*) $A = 11111000$.

15.66 Considere um circuito lógico L com $n = 6$ entradas, A, B, C, D, E, F, ou, equivalentemente, considere uma expressão booleana E com seis variáveis x_1, x_2, x_3, x_4, x_5, x_6.

(*a*) De quantas maneiras diferentes se pode atribuir um *bit* (0 ou 1) a cada uma das seis variáveis?

(*b*) Ache as três primeiras seqüências especiais para as variáveis (entradas).

15.67 Ache a tabela-verdade $T = T(E)$ para a expressão booleana $E = E(x, y, z)$ onde

(*a*) $E = xy + x'z$. (*b*) $E = xyz' + y + xy'$.

15.68 Ache a tabela-verdade $T = T(E)$ para a expressão booleana $E = E(x, y, z)$ onde

(*a*) $E = x'yz' + x'y'z$. (*b*) $E = xyz' + xy'z' + x'y'z'$.

15.69 Ache a expressão booleana $E = E(x, y, z)$ correspondente às tabelas-verdade:

(*a*) $T(E) = 10001010$; (*b*) $T(E) = 00010001$; (*c*) $T(E) = 00110000$.

15.70 Ache todas as possíveis somas minimais para cada expressão booleana E dada pelos mapas de Karnaugh da Figura 15-36.

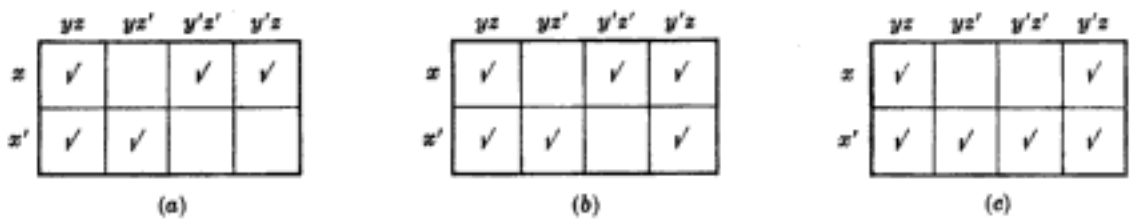


Fig. 15-36

15.71 Ache todas as possíveis somas minimais para cada expressão booleana E dada pelos mapas de Karnaugh da Figura 15-37.

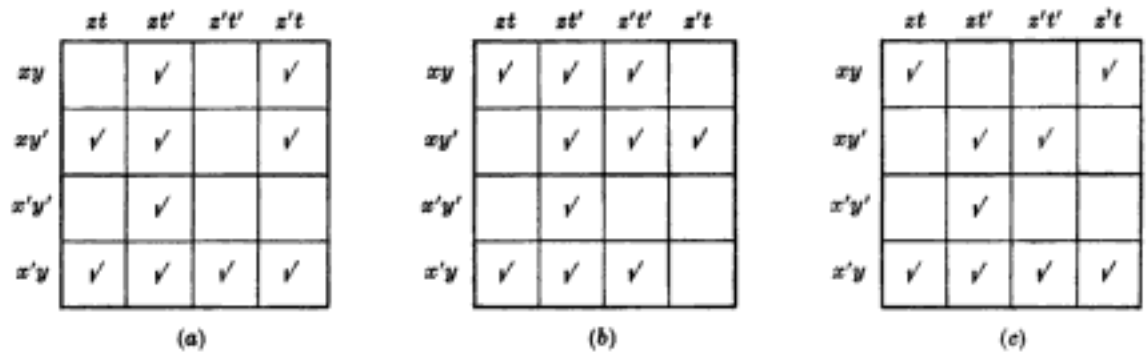


Fig. 15-37

15.72 Use um mapa de Karnaugh para achar uma soma minimal de cada expressão booleana.

(*a*) $E = xy + x'y + x'y'$. (*b*) $E = x + x'yz + xy'z'$.

15.73 Ache uma soma minimal para cada expressão booleana:

(*a*) $E = y'z + y'z't' + z't$. (*b*) $E = y'zt + xzt' + xy'z'$.

15.74 Use mapas de Karnaugh para reprojetar cada circuito lógico L da Figura 15-38 de forma que se transformem em circuitos minimais E-OU.

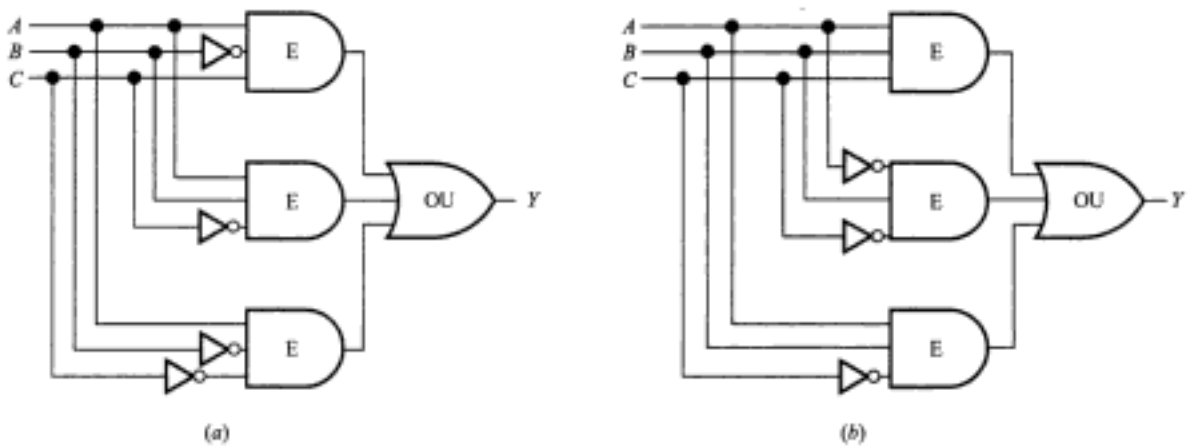


Fig. 15-38

15.75 Suponha que três interruptores A, B e C estejam conectados à mesma luz. A qualquer momento, um interruptor pode estar ligado, denotado por 1, ou desligado, denotado por 0. Uma mudança em qualquer interruptor altera a paridade (ímpar ou par) do número de 1s. Os interruptores controlarão a luz se for associada alguma paridade, por exemplo, ímpar à luz ligada (representado por 1) e par à luz desligada (representado or 0).

(*a*) Mostre que a seguinte tabela-verdade satisfaz estas condições.

$$T(A, B, C) = T(00001111, 00110011, 01010101) = 01101001$$

(*b*) Desenhe um circuito L, do tipo E-OU, com a tabela-verdade acima.

Respostas dos Problemas Complementares

15.43 (*a*) $a + a'b = a + b$.
(*b*) $a \cdot 0 + a \cdot 1 = a$.
(*c*) $ab + bc = (a + c)b$.

15.45 (*b*) $\mathbf{D}_{55}$; átomos 5 e 11; (*d*) $\mathbf{D}_{130}$; átomos 2, 5 e 13

15.46 (*a*) Existem oito elementos, 1, 2, 5, 10, 11, 22, 55, 110. Veja a Figura 15-39(*a*).
(*b*) Existem cinco subálgebras: {1, 110}, {1, 2, 55, 110}, {1, 5, 22, 110}, {1, 10, 11, 110}, $\mathbf{D}_{110}$.
(*c*) Existem 15 sub-reticulados que incluem as três subálgebras acima.
(*d*) $A = \{2, 5, 11\}$
(*e*) Veja a Figura 15-39(*b*).

Fig. 15-39

15.48 Termos máximos: 30, 42, 70, 105

15.49 (*b*) *Sugestão*: use dualidade.

15.53 (*a*) $xy'z$; (*b*) 0; (*c*) $xy'z't$; (*d*) 0

15.54 (*a*) $E = xy' + xy'z = xy'z' + xy'z$
(*b*) $E = xy + xz' = xyz + xyz' + xy'z'$
(*c*) $E = xy' + y'z = xy'z + xy'z' + x'y'z$

15.55 (*a*) $E = xyz' + x'y' = xyz' + x'y'z + x'y'z'$
(*b*) $E = x'y' = x'y'z + x'y'z'$
(*c*) $E = x'yz'$

15.56 (*a*) $Q = xzt$. (*b*) $Q = xyt'$. (*c*) e (*d*) Não existe.

15.57 (*a*) $E_L = 11$, $E_S = 3$ (*b*) $E_L = 11$, $E_S = 4$

15.58 (*a*) $x'y$, $x'z'$, $y'z'$
(*b*) xy', xzt', $y'zt'$, $x'z't$, $y'z't$
(*c*) $xyzt$, $xz't'$, $y'z't'$, $x'y'z'$, $x'z't$

15.59 (*a*) $E = x'y + x'z'$
(*b*) $E = xy' + xzt' + x'z't + y'z't$
(*c*) $E = xyzt + xz't' + x'y'z' + x'z't$

15.60 (*a*) $Y = A'BC + A'C' + BC'$; (*b*) $A + B + C + A'BC + AB'C'$

15.61 (*a*) $Y = (AB')' + (A' + B + C)' + AC$

(*b*) $Y = (A'BC)' + A'BC' + (AB'C)' + AB'C'$

15.62 Veja a Figura 15-40.

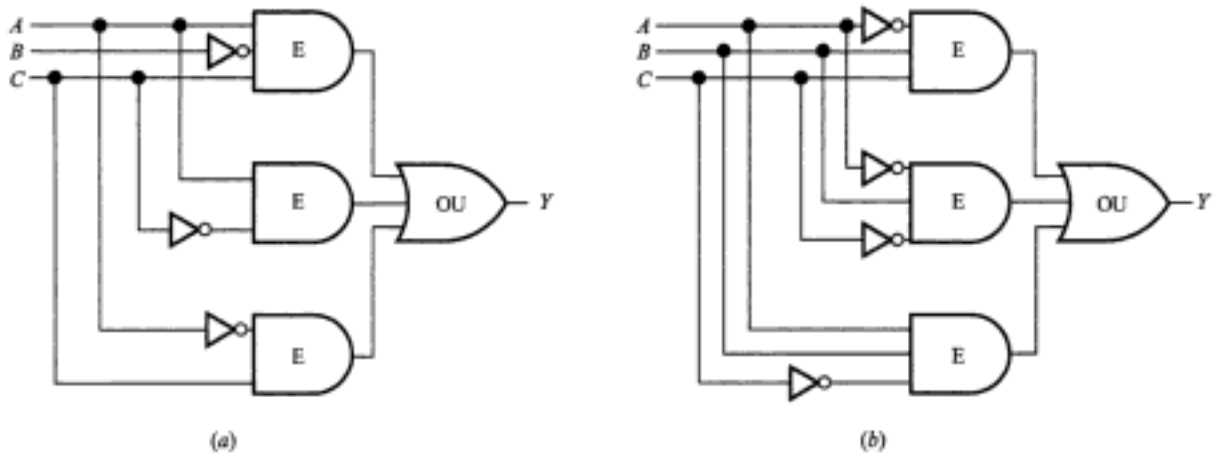


Fig. 15-40

15.63 (*a*) $Y = 100001$; (*b*) $Y = 00111000$; (*c*) $Y = 00110000$

15.64 (*a*) $Y = 100111$; (*b*) $Y = 10100111$; (*c*) $Y = 11111101$

15.65 (*a*) $A' = 00011000$; (*b*) $A' = 01110111$; (*c*) $A' = 00000111$

15.66 (*a*) $2^n = 2^6 = 64$

(*b*) $x_1 = 000\cdots00111 \cdot 11$ (32 zeros) (32 uns)

$x_2 = (00000000000000000111111111111111)^2$

$x_3 = (00000000111111111)^4$

15.67 (*a*) $T(E) = 01010011$; (*b*) $T(E) = 00111111$

15.68 (*a*) $T(E) = 01000000$; (*b*) $T(E) = 10001010$

15.69 Use tabelas-verdade para termos completos no Exemplo 15-13.

(*a*) $E = x'y'z' + xyz' + xyz'$

(*b*) $E = xy'z' + xyz$

(*c*) $E = x'yz' + xy'z'$

15.70 (*a*) $E = xy' + x'y + yz = xy' + x'y + xz'$

(*b*) $E = xy' + x'y + z$

(*c*) $E = x' + z$

15.71 (*a*) $E = x'y + zt' + xz't + xy'z = x'y + zt' + xz't + xy't$

(*b*) $E = yz + yt' + zt' + xy'z'$

(*c*) $E = x'y + yt + xy't' + x'zt = x'y + yt + xy't' + y'zt$

15.72 (*a*) $E = x' + y$; (*b*) $E = xz' + yz$

15.73 (*a*) $E = y' + z't$; (*b*) $E = xy' + zt' + y'zt$

Hidden page

Apêndice A

Relações de Recorrência

A.1 INTRODUÇÃO

Discutimos previamente (Seção 3.6) funções definidas recursivamente tais como:
(*a*) função fatorial, (*b*) seqüência de Fibonacci, (*c*) função de Ackermann.

Este apêndice discute certos tipos de seqüências $\{a_n\}$ definidas recursivamente e suas soluções. Uma seqüência é simplesmente uma função cujo domínio é

$$\mathbf{N} = \{1, 2, 3, \ldots\} \text{ ou } \mathbf{N}_0 = \mathbf{N} \cup \{0\}) = \{0, 1, 2, 3, \ldots\}$$

Começamos com alguns exemplos.

Exemplo A.1 Considere a seguinte seqüência que começa com o número 3, e cada um dos termos seguintes é obtido pela multiplicação por 2 do termo anterior:

$$3, 6, 12, 24, 48, \ldots$$

Ela pode ser definida recursivamente como

$$a_0 = 3, a_k = 2a_{k-1} \text{ para } k \geq 1 \quad \text{ou} \quad a_0 = 3, a_{k+1} = 2a_k \text{ para } k \geq 0$$

(A segunda definição pode ser obtida a partir da primeira fazendo $k = k + 1$.) Claramente, a fórmula $a_n = 3(2^n)$ nos dá o n-ésimo termo da seqüência sem que seja necessário calcular qualquer termo prévio. Devem ser feitas as seguintes observações:

(1) A equação $a_k = 2a_{k-1}$ ou, equivalentemente, $a_{k+1} = 2a_k$, onde um termo da seqüência é definido em função dos termos anteriores da seqüência, é chamada de *relação de recorrência*.

(2) A equação $a_0 = 3$, que atribui um valor específico a um dos termos, é dita a *condição inicial*.

(3) A função $a_n = 3(2^n)$, que dá uma fórmula para a_n como função de n, e não dos termos prévios, é dita a *solução* da relação de recorrência[†].

[†] N. de T. Essa nomenclatura não é muito utilizada em textos de matemática em português.

(4) Podem existir muitas seqüências satisfazendo uma relação de recorrência dada. Por exemplo,

$$1, 2, 4, 8, 16, \ldots \quad \text{e} \quad 7, 14, 28, 56, 112, \ldots$$

são soluções da relação recursiva $a_k = 2a_{k-1}$. Todas essas soluções formam a *solução geral* da relação de recorrência.

(5) Por outro lado, só pode existir uma única solução para uma relação recursiva que também satisfaz uma condição inicial dada. Por exemplo, a condição inicial $a_0 = 3$ produz unicamente a solução 3, 6, 12, 24,... da relação de recorrência $a_k = 2a_{k-1}$.

Este Apêndice nos mostra como resolver certas relações de recorrência. Apresentamos primeiramente duas seqüências importantes que, possivelmente, já foram estudadas pelo leitor.

Exemplo A.2

(*a*) *Progressão aritmética*
Uma progressão aritmética é uma seqüência da forma

$$a, a + d, a + 2d, a + 3d, \ldots$$

Isto é, a seqüência inicia com o número a e cada termo sucessivo é obtido a partir do termo prévio pela adição de d (a diferença comum entre quaisquer dois termos). Por exemplo,

(i) $a = 5, d = 3 : 5, 8, 9, 11, \ldots$
(ii) $a = 2, d = 5 : 2, 7, 12, 17, \ldots$
(iii) $a = 1, d = 0 : 1, 1, 1, 1, 1, \ldots$

Notamos que a progressão aritmética geral pode ser recursivamente definida por:

$$a_1 = a \text{ e } a_{k+1} = a_k + d \text{ para } k \geq 1$$

onde a solução é $a_n = a + (n - 1)d$.

(*b*) *Progressão geométrica*
Uma progressão geométrica é uma seqüência da forma

$$a, ar, ar^2, ar^3, \ldots$$

Isto é, a seqüência começa com um número a e cada termo sucessivo é obtido a partir do termo prévio pela multiplicação por r (a razão comum entre quaisquer dois termos). Por exemplo,

(i) $a = 1, r = 3 : 1, 3, 9, 27, 81, \ldots$
(ii) $a = 5, r = 2 : 5, 10, 20, 40, \ldots$
(iii) $a = 1, r = \frac{1}{2} : 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots$

Notamos que a progressão geométrica geral pode ser recursivamente definida por:

$$a_1 = a \text{ e } a_{k+1} = ra_k \text{ para } k \geq 1$$

onde a solução é $a_{n+1} = ar^n$.

A.2 RELAÇÕES DE RECORRÊNCIA LINEARES COM COEFICIENTES

CONSTANTES

Uma *relação de recorrência* de *ordem k* é uma função da forma

$$a_n = \Phi(a_{n-1}, a_{n-2}, \ldots, a_{n-k}, n)$$

isto é, onde o n-ésimo termo a_n da seqüência é uma função dos k termos precedentes (e, possivelmente, de n). Em particular, uma *relação de recorrência de ordem k com coeficientes constantes* é uma relação de recorrência da forma

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_k a_{n-k} + f(n)$$

onde $C_1, C_2, \ldots, C_k$ são constantes com $C_k \neq 0$, e $f(n)$ é uma função de n. O sentido da terminologia "linear" e "coeficientes constantes" é:

linear: não existem potências ou produtos de $a_j's$;

coeficientes constantes: os $C_1, C_2, \ldots, C_k$ são constantes (não dependem de n).

Se $f(n) = 0$, a relação também é dita homogênea.

Claramente, podemos resolver de maneira única para a_n se conhecemos os valores $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. Conseqüentemente, por indução matemática, existe uma única seqüência satisfazendo a relação de recorrência se são dados os *valores iniciais* para os primeiros k elementos da seqüência.

Exemplo A.3 Considere cada uma das seguintes relações de recorrência:

(*a*) $a_n = 5a_{n-1} - 4a_{n-2} + n^2$

Esta é uma relação de recorrência de segunda ordem com coeficientes constantes. Não é homogênea por causa de n^2. Suponha que são dadas as condições iniciais $a_1 = 1, a_2 = 2$. Podemos, então, achar seqüencialmente os próximos elementos da seqüência:

$$a_3 = 5(2) - 4(1) + 3^2 = 15, a_4 = 5(15) - 4(2) + 4^2 = 83$$

(*b*) $a_n = 2a_{n-1}a_{n-2} + n^2$

O produto $a_{n-1}a_{n-2}$ significa que a relação de recorrência não é linear. Dadas as condições iniciais $a_1 = 1, a_2 = 2$, podemos ainda assim achar os próximos elementos da seqüência:

$$a_3 = 2(2)(1) + 3^2 = 13, a_4 = 2(13)(2) + 4^2 = 68$$

(*c*) $a_n = na_{n-1} + 3a_{n-2}$

Esta é uma relação de recorrência linear de segunda ordem mas sem coeficientes constantes, porque o coeficiente de a_{n-1} é n, não uma constante. Dadas as condições iniciais $a_1 = 1, a_2 = 2$, os elementos seguintes da seqüência são

$$a_3 = 3(2) + 3(1) = 9, a_4 = 4(9) + 3(2) = 42$$

(*d*) $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$

Esta é uma relação de recorrência linear de terceira ordem com coeficientes constantes. Logo, precisamos de três e não duas condições iniciais para produzir uma solução única para a relação. Suponha que são dadas as condições iniciais $a_1 = 1, a_2 = 2, a_3 = 1$. Então, os elementos seguintes da seqüência são

$$a_4 = 2(1) + 5(2) - 6(1) = 6, a_5 = 2(2) + 5(1) - 6(6) = -37,$$
$$a_6 = 2(1) + 5(6) - 6(-37) = 254$$

Este apêndice investigará as soluções de relações de recorrência lineares homogêneas com coeficientes constantes. A teoria de relações de recorrência não homogêneas ou sem coeficientes constantes está além dos objetivos deste texto.

Por conveniência computacional, a maioria das nossas seqüências iniciará com a_0, e não com a_1. A teoria não é afetada por esta escolha.

A.3 RESOLUÇÃO DE RELAÇÕES DE RECORRÊNCIA LINEARES HOMOGÊNEAS

Considere uma relação de recorrência homogênea de segunda ordem com coeficientes constantes que tem a forma

$$a_n = sa_{n-1} + ta_{n-2} \text{ or } a_n - sa_{n-1} - ta_{n-2} = 0$$

onde s e t são constantes com $t \neq 0$. Associamos o polinômio quadrático seguinte com a relação de recorrência acima:

$$\Delta(x) = x^2 - sx - t$$

Este polinômio $\Delta(x)$ é dito o *polinômio característico* da relação de recorrência, e as raízes de $\Delta(x)$ são chamadas *raízes características*.

Valem os seguintes teoremas.

Teorema A.1: suponha que o polinômio característico

$$\Delta(x) = x^2 - sx - t \text{ da relação de recorrência}$$

$$a_n = sa_{n-1} + ta_{n-2}$$

tem raízes reais distintas r_1 e r_2. Então, a solução geral da relação de recorrência é

$$a_n = c_1 r_1^n + c_2 r_2^n$$

onde c_1 e c_2 são constantes arbitrárias.

Enfatizamos que as constantes c_1 e c_2 são unicamente determinadas pelas condições iniciais. Observamos que o teorema é verdade mesmo quando as raízes não são reais. Esses casos estão além dos objetivos deste texto.

Exemplo A.4 Considere a seguinte relação de recorrência homogênea:

$$a_n = 2a_{n-1} + 3a_{n-2}$$

A solução geral é obtida pela determinação do polinômio característico $\Delta(x)$ e suas raízes r_1 e r_2:

$$\Delta(x) = x^2 - 2x - 3 = (x-3)(x+1); \text{ raízes } r_1 = 3, r_2 = -1$$

Como as raízes são distintas, podemos usar o Teorema A.1 para obter a solução geral:

$$a_n = c_1 3^n + c_2(-1)^n$$

Assim, quaisquer valores para c_1 e c_2 darão a solução para a relação de recorrência.

Suponha que também nos seja dada a condição inicial $a_0 = 1, a_1 = 2$. Usando a relação de recorrência, podemos computar os seguintes termos da seqüência:

$$1, 2, 8, 28, 100, 356, 1268, 3516, \ldots$$

A solução única é obtida com a determinação de c_1 e c_2 usando as condições iniciais. Especificamente,

Para $n = 0$, $a_0 = 1 : c_1 3^0 + c_2(-1)^0 = 1$ ou $c_1 + c_2 = 1$.
Para $n = 1$, $a_1 = 2 : c_1 3^1 + c_2(-1)^1 = 2$ ou $3c_1 - c_2 = 2$.

Resolvendo o sistema de duas equações em c_1 e c_2, obtém-se:

$$c_1 = \frac{3}{4}, c_2 = \frac{1}{4}.$$

Portanto, a solução seguinte é a única solução da relação de recorrência dada com condições iniciais $a_0 = 1, a_1 = 2$:

$$a_n = \frac{3}{4}3^n + \frac{1}{4}(-1)^n = \frac{3^{n+1} + (-1)^n}{4}$$

Exemplo A.5 Considere a famosa seqüência de Fibonacci:

$$a_n = a_{n-1} + a_{n-2}, \text{ com } a_0 = 0, a_1 = 1$$

Os primeiros 10 termos da seqüência são

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Às vezes, a seqüência de Fibonacci é definida usando as condições iniciais $a_0 = 1, a_1 = 1$ ou as condições iniciais $a_1 = 1, a_2 = 2$. Usamos $a_0 = 0, a_1 = 1$ por conveniência computacional. (Todas as três condições produzem a mesma seqüência a partir dos termos 1, 2.)

Observe que a seqüência de Fibonacci é uma relação de recorrência consistente linear homogênea de segunda ordem e, portanto, pode ser resolvida usando o Teorema A.1. Seu polinômio característico é

$$\Delta(x) = x^2 - x - 1$$

Usando a fórmula quadrática, obtemos as raízes:

$$r_1 = \frac{1+\sqrt{5}}{2}, \quad r_2 = \frac{1-\sqrt{5}}{2}$$

Pelo Teorema A.1, obtemos a solução geral:

$$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

As condições iniciais originam o sistema seguinte de duas equações lineares em c_1 e c_2:

Para $n = 0$, $a_0 = 0$: $\quad 0 = c_1 + c_2$

Para $n = 1$, $a_0 = 1$: $\quad 1 = c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right)$

A solução do sistema é

$$c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}}$$

Conseqüentemente, a solução seguinte é a solução da relação de recorrência de Fibonacci:

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Pode-se mostrar que o valor absoluto do segundo termo para a_n acima é menor do que $1/2$. Logo, a_n também é o inteiro mais próximo de

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n \approx (0{,}4472)(1{,}6180)^n$$

Os valores aproximados dos primeiros termos na expressão acima são

$$0{,}4472, 0{,}7236, 1{,}1708, 1{,}8944, 3{,}0653, 4{,}99597, 8{,}0249, 12{,}9846, 21{,}0092$$

Suponha que as raízes do polinômio característico não sejam distintas. Neste caso, temos o resultado seguinte.

Teorema A.2: suponha que o polinômio característico

$$\Delta(x) = x^2 - sx - t \text{ da relação de recorrência}$$

$$a_n = sa_{n-1} + ta_{n-2}$$

tem apenas uma raiz r_0. Então, a solução da relação de recorrência é

$$a_n = c_1 r_0^n + c_2 n r_0^n$$

onde c_1 e c_2 são constantes arbitrárias.

Mais uma vez, observamos que as constantes c_1 e c_2 podem ser unicamente determinadas a partir das condições iniciais.

Exemplo A.6 Considere a seguinte relação de recorrência homogênea:

$$a_n = 6a_{n-1} - 9a_{n-2}$$

O polinômio característico $\Delta(x)$ é

$$\Delta(x) = x^2 - 6x + 9 = (x-3)^2$$

Logo, $\Delta(x)$ tem apenas uma raiz $r_0 = 3$. Agora use o Teorema A.2 para obter a seguinte solução para a relação de recorrência:

$$a_n = c_1 3^n + c_2 n 3^n$$

Logo, quaisquer valores de c_1 e c_2 darão uma solução para relação de recorrência.

Suponha que também nos são dadas as condições iniciais $a_1 = 3, a_2 = 27$. Usando a relação de recorrência, podemos computar os valores seguintes da seqüência:

$$3, 27, 135, 567, 2187, 8109, \ldots$$

A solução única é obtida usando as condições iniciais para determinar c_1 e c_2. Especificamente,

Para $n = 1, a_1 = 3$: $\quad 3 = c_1 3^1 + c_2(1)(3)^1$ ou $3c_1 + 3c_2 = 3$
Para $n = 2, a_2 = 27$: $\quad 27 = c_1 3^2 + c_2(2)(3)^1$ ou $9c_1 + 18c_2 = 27$

Resolvendo o sistema com as duas equações para c_1 e c_2, obtém-se:

$$c_1 = -1, c_2 = 2$$

Assim, a solução seguinte é a única solução da relação de recorrência dada com condições iniciais $a_1 = 3, a_2 = 27$:

$$a_n = -3^n + 2n3^n = 3^n(2n-1)$$

A.4 RESOLUÇÃO DE RELAÇÕES LINEARES DE RECORRÊNCIA GENÉRICAS

Considere agora uma relação linear de recorrência de ordem k genérica da forma

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + C_3 a_{n-3} + \ldots + C_k a_{n-k} = \sum_{i=1}^{k} C_i a_{n-i} \tag{A.1}$$

onde $C_1, C_2, \ldots, C_k$ são constantes com $C_k \neq 0$. O *polinômio característico* $\Delta(x)$ da relação de recorrência (A.1) é

$$\Delta(x) = x^k - C_1 x^{k-1} - C_2 x^{k-2} - C_3 x^{k-3} - \ldots - C_k = x^k - \sum_{i=1}^{k} C_i x^{k-i}$$

As raízes de $\Delta(x)$ são chamadas de *raízes características* da relação de recorrência.

As observações seguintes são pertinentes.

Observação 1: se $p(n)$ e $q(n)$ são soluções de (A.1), qualquer combinação linear

$$c_1 p(n) + c_2 q(n)$$

de $p(n)$ e $q(n)$ também é solução. (Isto não é verdade se a relação de recorrência não for homogênea.)

Observação 2: se r é uma raiz de multiplicidade m do polinômio característico $\Delta(x)$ de (A.1), então cada uma das seguintes

$$r^n, nr^n, n^2 r^n, \ldots, n^{m-1} r^n$$

é uma solução de (A.1). Logo, qualquer combinação linear

$$\begin{aligned} &c_1 r^n + c_2 n r^n + c_3 n^2 r^n + \ldots + c_m n^{m-1} r^n \\ &= (c_1 + c_2 n + c_3 n^2 + \ldots + c_m n^{m-1}) r^n \end{aligned}$$

também é solução.

Exemplo A.7 Considere a seguinte relação de recorrência homogênea de terceira ordem:

$$a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$$

O polinômio característico $\Delta(x)$ da relação de recorrência é

$$\Delta(x) = x^3 - 11x^2 + 39x - 45 = (x-3)^2(x-5)$$

Existem duas raízes $r_1 = 3$ de multiplicidade 2 e $r_2 = 5$ de multiplicidade 1. Logo, pelas observações acima, a solução geral da relação de recorrência é

$$a_n = c_1(3^n) + c_2n(3^n) + c_3(5^n) = (c_1 + c_2n)(3^n) + c_3(5^n)$$

Suponha que as seguintes condições iniciais são dadas: $a_0 = 5, a_1 = 11, a_2 = 25$. Os termos seguintes da seqüência são

$$5, 11, 25, 71, 301, 1667, \ldots$$

A solução única do sistema é obtida determinando os valores de c_1, c_2, c_3 usando as condições iniciais. Especificamente,

Para $n = 1, a_0 = 5$: $\quad c_1 + c_3 = 5$
Para $n = 1, a_1 = 11$: $\quad 3c_1 + 3c_2 + 5c_3 = 11$
Para $n = 2, a_2 = 25$: $\quad 9c_1 + 18c_2 + 25c_3 = 25$

Resolvendo o sistema de três equações em c_1, c_2, c_3, tem-se

$$c_1 = 4, c_2 = -2, c_3 = 1$$

Logo, a solução única da relação de recorrência com as condições iniciais dadas é

$$a_n = (4 - 2n)(3^n) + 5^n$$

Exemplo A.8 Considere a seguinte relação de recorrência homogênea de terceira ordem:

$$a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$$

O polinômio característico $\Delta(x)$ da relação de recorrência é

$$\Delta(x) = x^3 - 6x^2 + 12x - 8 = (x-2)^3$$

$\Delta(x)$ tem exatamente uma raiz $r_0 = 2$ de multiplicidade 3. Logo, a solução geral da relação de recorrência é

$$a_n = c_1(2^n) + c_2n(2^n) + c_3n^2(2^n) = (c_1 + c_2n + c_3n^2)2^n$$

Suponha que as seguintes condições iniciais são dadas: $a_0 = 3, a_1 = 4, a_2 = 12$. Então, podemos achar os valores de c_1, c_2, c_3. Especificamente,

Para $n = 0, a_0 = 3$: $\quad c_1 = 3$
Para $n = 1, a_1 = 4$: $\quad 2c_1 + 2c_2 + 2c_3 = 4$
Para $n = 2, a_2 = 12$: $\quad 4c_1 + 8c_2 + 16c_3 = 12$

Resolvendo o sistema de três equações em c_1, c_2, c_3, tem-se

$$c_1 = 3, c_2 = -2, c_3 = 1$$

Logo, a solução única da relação de recorrência com as condições iniciais dadas é

$$a_n = (3 - 2n + n^2)(2^n)$$

Observação: determinar as raízes do polinômio característico $\Delta(x)$ é um passo importante para resolver relações de recorrência. No caso geral, isto pode ser difícil quando a ordem k é maior do que 2. (O Exemplo 12.17 indica uma maneira de achar as raízes de alguns polinômios de grau maior ou igual a 3.)

Problemas Complementares

Relações de Recorrências Lineares Homogêneas com Coeficientes Constantes

A.1 Ache o polinômio característico $\Delta(x)$ e a solução geral de cada relação de recorrência:

(*a*) $a_n = 3a_{n-1} + 10a_{n-2}$ (*c*) $a_n = 3a_{n-1} - 2a_{n-2}$ (*e*) $a_n = 3a_{n-1} - a_{n-2}$

(*b*) $a_n = 4a_{n-1} + 21a_{n-2}$ (*d*) $a_n = 5a_{n-1} - 6a_{n-2}$ (*f*) $a_n = 5a_{n-1} - 3a_{n-2}$

A.2 Dadas as condições iniciais a seguir, ache a solução única de cada relação de recorrência do Problema A.1:

(*a*) $a_0 = 5, a_1 = 11$ (*c*) $a_0 = 5, a_1 = 8$ (*e*) $a_0 = 0, a_1 = 1$

(*b*) $a_0 = 9, a_1 = 13$ (*d*) $a_1 = 2, a_2 = -8$ (*f*) $a_0 = 0, a_1 = 1$

A.3 Ache o polinômio característico $\Delta(x)$ e a solução geral de cada relação de recorrência:

(*a*) $a_n = 6a_{n-1}$ (*b*) $a_n = 7a_{n-1}$ (*c*) $a_n = 4a_{n-1} - 4a_{n-2}$ (*d*) $a_n = 10a_{n-1} - 25a_{n-2}$

A.4 Dadas as condições iniciais a seguir, ache a solução única de cada relação de recorrência do Problema A.1:

(*a*) $a_0 = 5$ (*b*) $a_1 = 5$ (*c*) $a_0 = 1, a_1 = 8$ (*d*) $a_0 = 2, a_1 = 15$

A.5 Ache o polinômio característico $\Delta(x)$ e a solução geral de cada relação de recorrência:

(*a*) $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ (*b*) $a_n = 11a_{n-1} - 39a_{n-2} + 45a_{n-3}$

A.6 Ache a solução única da cada relação de recorrência com as condições iniciais:

(*a*) $a_n = 10a_{n-1} - 32a_{n-2} + 32a_{n-3}$ com $a_0 = 5, a_1 = 18, a_2 = 78$

(*b*) $a_n = 9a_{n-1} - 27a_{n-2} + 27a_{n-3}$ com $a_0 = 5, a_1 = 24, a_2 = 117$

Problemas Variados

A.7 Considere a seguinte relação de recorrência de segunda ordem e seu polinômio característico $\Delta(x)$:

$$a_n = sa_{n-1} + ta_{n-2}, \Delta(x) = x^2 - sx - t \qquad (*)$$

(*a*) Suponha que $p(n)$ e $q(n)$ são soluções de $(*)$. Mostre que $c_1p(n) + c_2q(n)$ também é solução de $(*)$ para quaisquer c_1 e c_2 constantes.

(*b*) Suponha que r é uma raiz de $\Delta(x)$. Mostre que $a_n = r^n$ também é uma solução de $(*)$

A.8 Suponha que r é uma raiz dupla de $\Delta(x) = x^2 - sx - t$.

(*a*) Mostre que $s = 2r$ e $t = -r^2$.

(*b*) Mostre que $a_n = nr^n$ também é uma raiz de $(*)$.

A.9 Repita o Problema A.6 para uma relação de recorrência linear de ordem k qualquer com coeficientes constantes da forma:

$$a_n = C_1a_{n-1} + C_2a_{n-2} + \ldots + C_ka_{n-k} = \sum_{i=1}^{k} C_ia_{n-i}$$

com polinômio característico $\Delta(x) = x^k - \sum C_ix^{k-i}$.

Respostas dos Problemas Complementares

A.1 (*a*) $\Delta(x) = x^2 - 3x - 10, a_n = c_1(5^n) + c_2(-2)^n$

(*b*) $\Delta(x) = x^2 - 4x - 21, a_n = c_1(7^n) + c_2(-3)^n$

(*c*) $\Delta(x) = x^2 - 3x + 2, a_n = c_1 + c_2(2^n)$

(*d*) $\Delta(x) = x^2 - 5x + 6, a_n = c_1(2^n) + c_2(3^n)$

(*e*) $\Delta(x) = x^2 - 3x + 1, a_n = c_1[(3 + \sqrt{5})/2]^n + c_2[(3 - \sqrt{5})/2]^n$

(*f*) $\Delta(x) = x^2 - 5x + 3, a_n = c_1[(5 + \sqrt{13})/2]^n + c_2[(5 - \sqrt{13})/2]^n$

A.2 (*a*) $a_n = 3(5^n) + 2(-2)^n$ (*b*) $a_n = 4(7^n) + 5(-3)^n$
(*c*) $a_n = 2 + 3(2^n)$ (*d*) $a_n = 7(2^n) - 4(3^n)$
(*e*) $a_n = \frac{1}{\sqrt{5}}\left(\frac{3+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{3-\sqrt{5}}{2}\right)^n$
(*f*) $a_n = \frac{1}{\sqrt{13}}\left(\frac{5+\sqrt{13}}{2}\right)^n - \frac{1}{\sqrt{13}}\left(\frac{5-\sqrt{13}}{2}\right)^n$

A.3 (*a*) $\Delta(x) = x - 6, a_n = c_1(6^n)$
(*b*) $\Delta(x) = x - 7, a_n = c_1(7^n)$
(*c*) $\Delta(x) = x^2 - 4x + 4, a_n = c_1(2^n) + c_2 n(2^n) = (c_1 + nc_2)2^n$
(*d*) $\Delta(x) = x^2 - 10x + 25, a_n = c_1(5^n) + c_2 n(5^n) = (c_1 + nc_2)5^n$

A.4 (*a*) $a_n = 5(6^n)$ (*c*) $a_n = (2^n) + 3n(2^n) = (1 + 3n)2^n$
(*b*) $a_n = 5(7^{n-1})$ (*d*) $a_n = 2(5^n) + n(5^n) = (2 + n)5^n$

A.5 (*a*) $\Delta(x) = x^3 - 5x^2 + 11x - 6, a_n = c_1 + c_2(2^n) + c_3(3^n)$
(*b*) $\Delta(x) = x^3 - 11x^2 + 39x - 45, a_n = c_1(3^n) + c_2 n(3^n) + c_3(5^n)$

A.6 (*a*) $a_n = 2(4^n) + n(4^n) + 3(2^n)$
(*b*) $a_n = 5(3^n) + 2n(3^n) + n^2(3^n) = (5 + 2n + n^2)3^n$

A.7 (*a*) Foi dado que $p(n)$ e $q(n)$ são soluções de $(*)$. Portanto,

$$p(n) = sp(n-1) + tp(n-2) \quad \text{e} \quad q(n) = sq(n-1) + tq(n-2)$$

Então,

$$\begin{aligned} c_1p(n) + c_2q(n) &= c_1[sp(n-1) + tp(n-2)] + c_2[sq(n-1) + tq(n-2)] \\ &= s[c_1p(n-1) + c_2q(n-1)] + t[c_1p(n-2) + c_2q(n-2)] \end{aligned}$$

Portanto, $c_1p(n) + c_2q(n)$ também é solução de $(*)$.

(*b*) Foi dito que r é uma raiz de $\Delta(x)$. Portanto,

$$r^2 - sr - t = 0 \quad \text{e} \quad r^2 = sr + t$$

Seja $a_n = r^n$. Então,

$$\begin{aligned} sa_{n-1} + ta_{n-2} &= sr^{n-1} + tr^{n-2} = (sr + t)r^{n-2} \\ &= r^2(r^{n-2}) = r^n = a_n \end{aligned}$$

Logo, $a_n = r^n$ é uma solução de $(*)$.

A.8 (*a*) Foi dado que r é uma raiz dupla de $\Delta(x)$. Portanto,

$$\Delta(x) = (x - r)^2 = x^2 - 2rx + 2^2$$

Mas $\Delta(x) = x^2 - sx - t$. Logo, $s = 2r$ e $t = -r^2$.

(*b*) Seja $a_n = nr^n$. Então,

$$\begin{aligned} &sa_{n-1} + ta_{n-2} = s(n-1)r^{n-1} + t(n-2)r^{n-2} \\ &= 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} = 2(n-1)r^n - (n-2)r^n \\ &= r^n[2(n-1) - (n-2)] = r^n[2n - 2 - n + 2] = nr^n = a_n \end{aligned}$$

Logo, $a_n = r^n$ é uma solução de $(*)$.

Índice

Adjacente:
  produtos fundamentais, 468-469
  regiões, 203-204
  vértices, 190-191, 229-230
Álefe-zero, 67
Alfabeto, 387-388
Álgebra:
  booleana, 454-455
  de conjuntos, 16-17, 26
  de matrizes, 111-112
  de proposições, 87-88
  teorema fundamental da, 366-367
Algoritmo de Huffman, 282-283
  código, 284-285
Algoritmo de *pruning*, 247-248
Algoritmo de Warshall, 237-238
Algoritmo de Well-Powell, 202-203
Algoritmos, 68-72
  complexidade de, 70
  de divisão, 307-308, 326-327
  de Euclides, 69, 311, 364-365
Ancestral, 270
Anel, 360-363
  de polinômios, 362-367
Arcos, 229-230
Arcos paralelos, 231-232
Aresta, 190-191, 229-230
  paralela, 230
Argumentos, 14, 31, 89-90
Aritmética modular, 61, 325-326
Arquivo
  de aresta, 205-206, 241-242
  de vértice, 205-206, 241-242
Array, 104-105
Árvore, 197-198
  binária, *ver* Árvore binária
  de derivação, 395-396
  diagrama, 45-46
  enraizada, 232-233
    ordenada, 233-234
  geradora, 198-199
  geral, 285-286
Árvore binária, 268-269
  completa, 269-270
  estendida, 271
  similar, 269-270
Árvore binária de busca, 276
  complexidade de algoritmos, 277-278
Associados, 363-364
Átomos, 433-434
Atravessável:
  multigrafo, 195
  trilha, 195
AUT(⊇) (automorfismos), 356-357
Autômato, 390-391
  de pilha, 396-397
  linear limitado, 396-397
Automorfismo, 356-357
Axioma da escolha, 430-431

BFS (busca em largura), 208-209, 242-243
Binária:
  adição, 399-400
  busca, 71-72
  dígito, 118-119, 454-455
  operação, 349-350
  relação, 36-37
Binomial:
  coeficientes, 136-137
  distribuição, 161-162
Bits, 454-455
Booleano:
  álgebra, 454-463
  anel, 383-384
  expressão, 458
    minimal, 460
  função, 467-468
  matriz, 118-119, 235
  subálgebra, 455-456
Bubble-sort, 71-72
Busca:
  binária, 71-72
  em largura, 242-243
  em profundidade, 208-209, 242-243

$C(n, r)$ (combinações), 140-141
C, números complexos, 12-13
Cadeia, 423-424
Caminho em um grafo, 193, 231-232
  matriz, 236-237
  menor, 196
  mínimo, 196

simples, 193
Caminho fechado, 193, 231-232
Caminho mínimo, 196
algoritmo, 239-240
Campo, 360-361, 376-377
Cantor, 67
teorema, 67-68,79-80
Caroll, Lewis, 14
Caso médio, 69-70
Ciclo, 193, 231-232
hamiltoniano, 195
Circuito, 193, 231-232
E-OU, 464-465
hamiltoniano, 195
lógico, 462-463
Classe lateral, 356-357
Classes de conjuntos, 19-20, 27
resíduos, 314-315
Cobertura minimal, 471
Código, 284-285
Huffman, 284-285
Codomínio, 56-57
Coloração:
grafos, 202-203
mapas, 220-221
Coluna, 106-107
Combinações, 139-140
Complemento:
em um conjunto, 15-16
em um reticulado,433-434
em uma álgebra booleana,454-455
Completo:
árvore binária, 270
forma de soma de produtos, 460
grafo, 196-197
Comp-lex ordem, 424-425
Complexidade de algoritmos, 69-70
em uma árvore binária de busca, 277-278
em uma *heap*, 277-278
Composição:
de funções, 58-59
de relações, 40
Comprimento:
de caminho, 193, 231-232
de um vetor, 105-106
de uma palavra, 387-388
Concatenação, 387-388
Conjunção, 84, 431
Conjunto, 11-21
álgebra de, 16-17
enumerável, 67-68
finito, 18-19
indexado, 63
ordenado, 422-423
produto, 35-36, 424-425
quociente, 43-44
Conjunto bem-ordenado, 428-429
princípio, 307-308
Conjunto de partes, 19-20, 27
Conjunto infinito, 67
Conjunto parcialmente ordenado, 44-45, 422-423
Conjunto totalmente ordenado, 423-424
Conjunto vazio, ∅, 12-13
árvore, 268-269
Conjuntos disjuntos, 15
Conjuntos indexados, 63-64
Consensus, 460-461
método, 461-462
Contradição, 86-87
Contra-exemplo, 95
Corte, 194
Crescimento de funções, razão de, 70-71
Cross partition, 31

$d(u, v)$ (distância), 194
Declaração bicondicional, 88-89
Declaração composta, 83-84
Declaração condicional, 88-89
Declaração contrapositiva, 98-99
Declaração conversa, 98-99
Decomposição redundante, 433-434
Descendente, 270
Desigualdades, 304-305, 322-323
Desvio-padrão, 162-163
Determinantes, 112-114
DFU (domínio de fatoração única), 363-364
Diagonal de uma matriz, 110-111
Diagrama:
de Hasse, 424-425
de Venn, 13-14, 23-24
estado, 391-392, 397-398
Diâmetro de um grafo, 194
Dígrafo (grafo orientado), 229-232
matriz de, 235
DIP (domínio ideal principal), 361-362
Disjunção (ou), 84-85
Disjunção, 430-431
irredutível por, 433-434
Distância entre vértices, 194
Distribuição, 161-162
binomial, 164-165
Divisão sintética, 68-69
Divisibilidade, 362-363
de inteiros, 308-309, 328-329
de polinômios, 363-364
$\mathbf{D}_n$, 455-456
Domínio:
de uma função, 56-57
de uma relação, 36-37
Domínio de fatoração única, 363-364
Domínio integral, 360-361

Dual:
  mapa, 203-204
  ordem, 422-423
Dualidade
  em um reticulado, 430-431
  em uma álgebra booleana, 455-456
  princípio da, 18-19, 26, 430-431, 455-456

$E(G)$ (arestas de um grafo), 190-191
Elemento de um conjunto, 11-12
Elemento irredutível:
  em um anel, 362-363
  em um reticulado, 433-434
Elemento unidade (identidade) em um anel, 361
Elementos comparáveis, 423-424
Eliminação gaussiana, 114, 127-128
Endereço, 233-234
Entrada (em uma máquina de Turing), 403-404
Enumeração consistente, 426, 438-439
Equipotente, 67
Equivalência:
  classe, 43-44
  relação, 42-43, 51, 53-54
Equivalência lógica, 87-88
Escalar, 19-20, 363-364
  multiplicação, 107-108
Espaço amostral, 154-155
Espaço equiprovável, 156-157, 166
Estado, 390-391, 401-402
  diagrama, 391-392, 397-398
  tabela, 397-398
Estados "sim", 390-391
Estados aceitáveis, 390-391
Estrutura de adjacências, 205-206, 241
Euler:
  fórmula, 200-201, 311
  função Phi, 316-317, 334
Evento (probabilidade), 127-128
  elementar, 154-155
  independente, 158-159, 171-172
Evento impossível, 154-155
Eventos mutuamente excludentes, 154-155
Expectância, 69-70, 162-163, 175-176
Expressão, 401-402
  algébrica, 269-270
  regular, 389-390
Extremos, 190-191

Fatorial, 65, 136-137
Fecho de Kleene, 424-425
Fecho de relações, 41-42, 48-49
  transitivo, 237-238
Fila de prioridades, 190-191, 277-278
Filhos, 270, 285-286
Finito:
  autômato de estados (AEF), 390-391, 408-409
  conjunto, 18-19, 25-26
  espaço de probabilidade, 155-156
  grafo, 191-192
  máquina de estados, 397-398
Fita (máquina de Turing), 399-400
  expressão, 401-402
Floresta, 197-198, 286-287
Fonte, 230-231
Forma de Backus-Naur, 396-397
Forma normal disjuntiva, 460
Forma paramétrica, 129-130
Forma pósfixa, 234
Forma triangular, 114-115
Função bijetiva, 59
Função *ceiling*, 60
Função computável, 404-406, 414-415
Função de Ackermann, 67
Função exponencial, 61
Função *floor*, 60
Função injetiva, 59
Função sobrejetora, 59
Função, 66-77
  computável, 404-406, 414-415
  definida recursivamente, 65, 77-78
  polinomial, 58-59
  próximo estado, 390-391
  razão de crescimento, 70-71
Funções logarítmicas, 62

Geradores de um grupo, 358-359
Gráfico de função, 57-58
Grafo, 188-189
  bipartidonados, 197-198
  completo, 196-197
  conexo, *ver* Grafo conexo
  de uma relação, 37-38
  estrutura de adjacências, 205-206, 240-241
  matriz de, 204-205
  orientado, 229-232
  planar, *ver* Grafo planar
  ponderado, 195-196
  regular, 196-197
  rotulado, *ver* Grafo rotulado
Grafo acíclico, 198-199, 245-246
Grafo bipartidonado, 197-198
Grafo conexo, 193
  componentes, 193
  fortemente, 231-232
  fracamente, 231-232
  mapa, 200-201
  unilateralmente, 231-232
Grafo denso, 204-205
Grafo estrela, 201-202
Grafo euleriano, 195
  trilha, 195
Grafo hamiltoniano, 195
  ciclo, 195
Grafo homeomorfo, 192

Grafo não planar, 201-202
Grafo orientado, 229-232
  de relações, 38-39
Grafo planar, 199-203
  coloração, 202-203
Grafo rotulado, 195-196
  dígrafo, 229-230
Grafo trivial, 191-192
Gramática, 393, 410-411
  tipos de, 395
Grau:
  de polinômio, 362-363
  de um vértice, 191-192, 230-231
  de uma região, 200-201
Grau de entrada, 230-231
Grau de saída, 230-231
Grupo, 355-356, 370
  cíclico, 358-359
  homomorfismos, 359-360
  quociente, 357-358
  simétrico, 356-357
Grupo abeliano, 355-356
Grupo diedral, 382-383

Heap, 278-282
Homomorfismo:
  de anéis, 362-363
  de grupos, 359-360
  de semigrupos, 354

Ideal, 361-362
Ideal principal, 361-362
Identidade:
  elemento, 351-352
  função, 57-58
  matriz, 110-111
  relação, 37-38
Igualdade:
  de conjuntos, 11-12
  de funções, 56-57
  de matrizes, 106-107
Imagem:
  de uma função, 56-57, 359-360
  de uma relação, 36-37
Implicação lógica, 91
Implicantes primos, 384, 460-461
I_n, matriz identidade, 110-111
Incidência, 190-191
Independentes:
  eventos, 158-159, 171-172
  tentativas repetidas, 152-153, 172-173
Índice de um subgrupo, 357-358
Indução matemática, 21-22, 306-307, 429-430
  transfinita, 429-430
Infimum (inf), 426-427, 439

Inteiros, 304-312
  módulo m, 315-316, 358-361
Inteiros positivos, $\mathbf{N}$, 12-13, 304-308
Interseção de conjuntos, 15, 20-21
Inversível:
  funções, 59, 73-74
  matrizes, 111-112
Inverso:
  elemento, 351-352
  função, 59
  matriz, 111-112, 118
  ordem, 422-423
  relação, 37-38
Isomorfo:
  álgebra booleana, 455-456
  anéis, 362-363
  conjuntos ordenados, 428-429
  grafos, 192
  grupos, 359-360
  reticulados, 432-433
  semigrupos, 298-299

Kernel(Ker), 359-360
Kleene, 392
  fecho, 392, 424-425
$\mathbf{K}_{m,n}$ (grafo biparticionado completo), 197-198
$\mathbf{K}_n$ (grafo completo), 196-197

Laço, 191-192, 230-231
Lei de absorção, 430-431
Lei de cancelamento, 352-353
  para congruências, 315-316
Lei do silogismo, 90-91
Leis de DeMorgan, 18, 20-21, 94, 456
Leis de idempotência, 18, 430-431
Lema de *pumping*, 393
Limitado:
  conjunto, 426-427
  reticulado, 432-433
Limite inferior, 426-427
Limite superior, 432-433
Linear:
  busca, 69-70, 71-72
  equações, 109-110, 117
  ordem, 423-424
Linguagem, 388-389, 406-407
  regular, 389-390, 395
  tipos de, 395
Linha (de matriz), 106-107
  equivalência, 114-115
  forma canônica, 114-115
  operações, 114, 127-128
  redução, 114
Lista, 63
  ligada, 188-189

Literal, 458
LNR percurso, 274
Lógica, 83-97, 462-463
  equivalência, 87-88
  implicação, 91
  operações, 84-85
Lógico, 83-97, 462-463
  circuitos, 462-463
  portas, 462-463
LRN percurso, 274

MAP(⊐), 356-357
Mapa, 200-201
  dual, 203-204
Mapas de Karnaugh, 468-473
Mapeamento de conjuntos, 56-57, 356-357
Mapeamento de similaridade, 428-429
Máquina:
  de estados finitos, 397-398
  de Turing, 401-402, 412-413
Matriz, 106-113
  aumentada, 110-111
  booleana, 31
  de adjacências, 204-205, 235
  de caminhos, 236-237
  de uma relação, 38-39
Matriz escalonada, 114-115, 127-128
Matriz não singular, 111-112
Matrizes, 106-113
  determinante de, 112-113
  inversa de, 111-112
  multiplicação, 108-109
  quadrado, 110-114
Maximal:
  elemento, 426
  ideal, 384
  retângulo, 471
Máximo divisor comum, 68-69, 310
mdc(a, b) (máximo divisor comum), 310
Média, 162-163, 177-178
Membro de um conjunto, 11-12
Merge-sort, 71-72
Método de Horner, 68-69
Minimal:
  árvore geradora, 198-199
  caminho, 195-196
  cobertura, 471
  elemento, 426
  expressões booleanas, 460
Mínimo múltiplo comum, 312
Modus Ponnens, 89-90
Monóide, 352-353
Multigrafo, 191-192

N (inteiros positivos), 12-13, 304-308
$n(\sqsupset)$ (número de elementos), 18-19
Negação, 85-86
  de um quantificador, 94
Nível, 66, 232-233
NLR percurso, 274
Nó terminal, 268-269
Norma, 105-106
Nós, 188-189, 229-230, 268-269
  externos, 271, 280-282
  internos, 269-270, 272-273, 280-282
Notação O, 70-71
Notação polonesa, 234
Núcleo, 359-360
Número cromático, 202-203
Número primo, 309-310
Números cardinais, 67-68, 75-76
  desigualdades, 67-68
Números complexos **C**, 12-13
Números de Gödel, 400-401

Operações, 349-350
  conjunto, 15, 22-23
Operações associativas, 350-351
Operações comutativas, 350-351
  grupo, 355-356
Ordem, 304-305, 422-423
  de um elemento, 358-359
  de um grupo, 355-356
  desigualdades, 304-305
  dual, 422-423
  em uma álgebra booleana, 456
Ordem lexicográfica, 234, 424-425
Ordem usual, 422-423
Ordenação topológica, 32-33
Ordenação parcial, 44-45, 422-423
Ordenado:
  árvores enraizadas, 233-234
  conjunto, 422-423
  par, 35-36
  partições, 142-143, 147-148

Pais, 270, 285-286
Palavra, 387-388
  vazia, 387-388
Partição:
  de um conjunto, 20-21, 31, 43-44, 51
  de um inteiro positivo, 425
  ordenada, 148-149
Percurso em pré-ordem, 274
Percurso em-ordem, 274
Percurso pós-ordem, 274
PERM(⊐), 356-357

Permutações, 138-139, 356-357
  com repetição, 139-140
Pilha, 190-191
Pior caso, 69-70
Pivô, 116-117
Polinômio, 362-367
  função, 58-59
  mônico, 362-363
  raízes de, 364-365
Ponderado:
  comprimento de caminho, 280-282
  grafo, 195-196
Ponte (em um grafo), 194
Ponteiro, 188-189
Porta E, 463-464
Porta lógica, 462-463
Porta NÃO, 463-466
Porta NE, 465-466
Porta OU, 462-463
Precede, 422-423
Premissas, 89-90
Primeiro elemento, 426
Primos relativos, 312
Princípio da abstração, 12-13
Princípio da casa do pombo, 141-142
Princípio da enumeração, 18-19, 135-136
Princípio da extensão, 11-12
Princípio da substituição, 87-88
Princípio de inclusão-exclusão, 141-142
Probabilidade, 154-165
  condicional, 157-158
Problema das pontes de Königsberg, 194
Produção em uma gramática, 394
Produto cartesiano, 35-36
Produto direto de grupos, 383-384
Produto escalar, 105-106
Produto:
  conjunto, 35-36
  direto, 383-384
  ordem, 424-425
  regra, 135-136
Produto fundamental, 16-17, 458
  adjacente, 468-469
Produto interno, 105-106
Profundidade,
  de uma árvore binária, 270
  de uma recursão, 66
Proposição, 83-87
  tabela-verdade de, 85-86
Proposicional:
  cálculo, 83-90
  função, 91

Q, (números racionais), 12-13
Quantificador existencial, 92
Quantificadores, 91-97
  negação de, 94
Quasi-ordem, 423-424
Quíntupla (máquina de Turing), 402-403
Quociente
  conjunto, 43-44
  grupo, 357-358
  semigrupo, 353-354
R (sistema de números reais) 12-13, 305-306
Raiz:
  de uma árvore binária, 268-269
  de uma árvore, 314-315
  de uma polinômio, 364-365
Razão de crescimento, 70-71
Real:
  reta **r**, 305-306
  sistema de números **R**, 12-13
Reconhecimento de palavras, 391-392
Região de um mapa, 200-201
Regra da soma, 135-136
Regular:
  expressão, 389-390
  grafo, 109-110
  gramática, 395-396
  linguagem, 389-390
Relação, 35-46
  congruência, *ver* Relação de congruência
  equivalência, 42-43
  fecho de, 41-42
  grafo de, 37-38
  matriz de, 38-39
Relação anti-simétrica, 41
Relação de congruência, 313-314, 332-333
  aritmética, 314-315
  equação, 317-318
Relação de igualdade, 37-38
Relação *n*-ária, 44-45
Relação reflexiva, 40
Relação ternária, 44-45
Relação transitiva, 41
  fecho de, 42-43
Relativamente primo, 316-317
Relativo:
  complemento, 15-16
  freqüência, 154-155
Representação computacional:
  de árvore binárias, 272
  de grafos orientados, 235
  de grafos, 204-205
Resto:
  função, 61
  teorema, 364-365
Retângulo básico, 470-471, 472
  maximal, 471
Reticulado, 430-433

Reticulado complementado, 433-434
Reticulado distributivo, 433-434

Semigrupo, 352-353
Semigrupo livre, 352-353, 388-389
  ordem, 424-425
Seqüências, 63
  Fibonacci, 66
Seqüência especiais, 466-467
Símbolo de somatório Σ, 63-64
Simétrica:
  diferença, 16-17
  grupo, 355-356
  matriz, 123-124
  relação, 41
Similar:
  árvores binárias, 269-270
  conjuntos ordenados, 428-429
Simples:
  caminho, 193, 235
  grafo, 191-192
Sistema reduzido de resíduos, 316-317
Soma de produtos, 458
  completa, 460
Strings, 63-64
Subárvore, 268-269
Subconjunto, 12-13
  próprio, 13-14
Subgrupo, 356-357
  normal, 357-358
Subpalavra, 387-388
Subsemigrupo, 353-354
Sucede, 422-423
Sucesso, 160
Sucessor, 229-230, 424-425
  lista, 211-212
Sumidouro, 230-231
Supremum (sup), 426-427

Tabelas-verdade, 85-86, 466-467
Tautologia, 86-87
Tentativas de Bernoulli, 160
Tentativas repetidas, 159-160, 172-173
Teorema chinês do resto, 320-321, 343
Teorema da fatoração, 364-365
Teorema das quatro cores, 203-204
Teorema de Apple-Haken, 203-204
Teorema de Kuratowski, 201-202
Teorema de Lagrange, 357-358
Teorema de Schroeder-Bernstein, 67-68, 79-80
Terminal em uma gramática, 393
Termo completo, 460
Termo máximo, 487-488
Transposta de matriz, 110-111
Triângulo de Pascal, 137-138
Trilha, 193
  atravessável, 195

Último elemento, 426
Um-a-um:
  correspondência, 59
  função, 58-59
União de conjuntos, 15
Unidade:
  em um anel, 360-361
  em uma álgebra booleana, 363-364
  matriz fórmula, 110-111
Unilateralmente conexo, 231-232
Universal:
  conjunto Universo, 12-13
  quantificadores, 92
  sistema de endereçamento, 233-234
Utility graph, 201-202

$V(G)$, 190-191
Valor absoluto, 60, 305-306
Valor base, 65
Valor inteiro, 60
Valores verdade, 83-84
Variância, 163-164
Variável, 56-57
  aleatória, 161-162
  em uma gramática, 394
Vazio:
  conjunto ∅, 12-13
  palavra, 387-388
  relação, 37-38
Vértice, 190-191, 229-230
  arquivo, 241-242
  isolado, 191-192
Vértice alcançável, 231-232
  matriz, 236-237
Vetores, 104-108
Vizinho, 240-241

$\mathbf{Z}$, (inteiros), 12-13, 304-305
$\mathbf{Z}_m$ (inteiros módulo m), 315-316
Zero:
  divisor, 360-361
  elemento, 454-455
  matriz, 106-107
  vetor, 105-106

IMPRESSÃO:
GRÁFICA EDITORA
Pallotti
Santa Maria - RS - Fone/Fax: (55) 3220.4500
www.pallotti.com.br

Coleção
SCHAUM

AYRES JR. & MENDELSON
Cálculo, 4.ed.

CARTER, N.
Arquitetura de Computadores

CATHEY, J.
Dispositivos e Circuitos Eletrônicos, 2.ed.

EDMINISTER, J.
Eletromagnetismo, 2.ed.

GUSTAFSON, D.
Engenharia de Software

HAYES, M.
Processamento Digital de Sinais

HSU, HWEI P.
Comunicação Analógica e Digital, 2.ed.

HSU, HWEI P.
Sinais e Sistemas

HUBBARD, J. R.
Programação em C++, 2.ed.

KAZMIER, L. J.
Estatística Aplicada à Administração e Economia, 4.ed.

LIPSCHUTZ & LIPSON
Álgebra Linear, 3.ed.

LIPSCHUTZ & LIPSON
Matemática Discreta, 2.ed.

MENDELSON, E.
Introdução ao Cálculo, 2.ed.

MOYER & AYRES JR.
Trigonometria, 3.ed.

NAHVI & EDMINISTER
Circuitos Elétricos, 4.ed.

RICH, B., revisado por P. A. SCHMIDT
Geometria, 3.ed.

ROSENBERG & EPSTEIN
Química Geral, 8.ed.

SAFIER, F.
Pré-cálculo

SCHMIDT & AYRES
Matemática para Ensino Superior, 3.ed.

SPIEGEL & LIU
Manual de Fórmulas e Tabelas Matemáticas, 2.ed.

SPIEGEL & MOYER
Álgebra, 2.ed.

SPIEGEL, SCHILLER & SRINIVASAN
Probabilidade e Estatística, 2.ed.

TITTEL, E.
Rede de Computadores

TITTEL, E.
XML

WREDE & SPIEGEL
Cálculo Avançado, 2.ed.

Bookman
www.bookman.com.br

Hidden page

Coleção
SCHAUM
A essência do conhecimento

Os livros da Coleção Schaum são estruturados de maneira que o aluno possa aprender a matéria e estudá-la de acordo com o seu ritmo. Além de apresentar o conteúdo essencial, atendo-se a tópicos fundamentais, os textos reúnem uma grande quantidade de exercícios, o que permite testar as habilidades adquiridas. Para o professor, é um material didático completo, com teoria, problemas resolvidos e complementares.

Teoria e Problemas de Matemática Discreta
aborda os seguintes tópicos:

- Teoria dos conjuntos
- Relações
- Funções e algoritmos
- Lógica e cálculo proposicional
- Vetores e matrizes
- Contagem
- Teoria das probabilidades
- Teoria dos grafos
- Grafos orientados
- Árvores binárias
- Propriedades dos inteiros
- Sistemas algébricos
- Linguagens, gramáticas e máquinas
- Conjuntos ordenados e reticulados
- Álgebra booleana
- Relações de recorrência

ISBN 978-85-363-0361-1
artmed®
EDITORA
RESPEITO PELO CONHECIMENTO
Bookman
www.bookman.com.br