

Elementos de Matemática Discreta para Computação

Anamaria Gomide

^

Jorge Stolfi

Versão Preliminar de 25 de agosto de 2011

© 2011

Sumário

Prefácio	11
1 Introdução à lógica matemática	15
1.1 Como ter certeza?	15
1.2 A invenção da lógica	15
1.3 Euclides e demonstrações geométricas	15
1.4 Álgebra	17
1.5 As linguagens da lógica matemática	17
2 Teoria dos Conjuntos	19
2.1 Especificando conjuntos	19
2.1.1 Definições circulares e contraditórias	20
2.2 Igualdade de conjuntos	20
2.3 Conjunto vazio	21
2.4 Relação de inclusão	21
2.5 Cardinalidade	21
2.6 Operações com conjuntos	21
2.6.1 União e intersecção	21
2.6.2 Diferença, universo, e complemento	22
2.6.3 Diferença simétrica	22
2.6.4 Propriedades das operações com conjuntos	23
2.7 Conjuntos de conjuntos	24
2.8 Conjunto potência	25
2.9 Partição	25
2.10 Produto cartesiano de dois conjuntos	25
2.10.1 Produto de dois conjuntos	25
2.11 Exercícios	26
3 Lógica matemática	27
3.1 Lógica proposicional	27
3.1.1 Proposições e valores lógicos	27
3.1.2 Conectivos lógicos e proposições compostas	28
3.1.3 Notação para cálculo proposicional	28
3.1.4 Operador de conjunção	29
3.1.5 Operador de disjunção	29

3.1.6	Operador de negação	29
3.1.7	Operador de implicação	30
3.1.8	Operador de equivalência	32
3.1.9	Operador de disjunção exclusiva	32
3.1.10	Precedência dos operadores lógicos	33
3.2	Afirmações auto-referentes	34
3.3	Manipulação lógica de proposições	36
3.3.1	Tautologias e contradições	36
3.3.2	Equivalência lógica	37
3.3.3	Equivalências lógicas importantes	37
3.3.4	Implicação lógica	40
3.3.5	Equivalência em contexto específico	41
3.4	Síntese de proposições	41
3.4.1	Formas normais disjuntivas e conjuntivas	41
3.4.2	Sistemas completos de operadores	42
3.5	Dualidade lógica	43
3.6	Lógica de Predicados	43
3.6.1	Quantificação universal	44
3.6.2	Quantificação existencial	45
3.6.3	Quantificador de existência e unicidade	46
3.6.4	Quantificação sobre o conjunto vazio	46
3.6.5	Cálculo de predicados	47
3.6.6	Negação de quantificadores	47
3.6.7	Distributividade de quantificadores	47
3.6.8	Traduzindo linguagem natural para proposições quantificadas	48
3.6.9	Mudança de domínio	50
3.6.10	Quantificadores múltiplos	51
3.6.11	Escopo de um quantificador	52
3.6.12	Omissão do domínio	52
4	Métodos de Prova de Teorema	55
4.1	Introdução	55
4.1.1	Definições	55
4.1.2	Conjeturas	56
4.2	Métodos de prova	57
4.3	Prova de implicações	57
4.3.1	Método direto	58
4.3.2	Método da contrapositiva	58
4.3.3	Método de redução ao absurdo	59
4.3.4	Implicação com tese conjuntiva	59
4.3.5	Implicação com hipótese disjuntiva	60
4.4	Prova de afirmações “se e somente se”	61
4.5	Prova de quantificador universal	62
4.5.1	Suspensão do quantificador	62
4.5.2	Prova por vacuidade	63

4.6	Prova de teoremas com o quantificador existencial	63
4.6.1	Demonstrações construtivas	63
4.6.2	Demonstrações não construtivas	65
4.6.3	Provas de existência e unicidade	65
4.6.4	Prova de falsidade por contra-exemplo	66
4.7	Exercícios	67
5	Indução Matemática	69
5.1	Introdução	69
5.2	Princípio de Indução Matemática	69
5.2.1	Formulação do PIM usando conjuntos	71
5.3	Generalizações da Indução Matemática	72
5.3.1	Base genérica	72
5.3.2	Passo genérico constante	74
5.4	Mais exemplos de indução matemática	75
5.5	Usos indevidos da indução matemática	77
5.6	Princípio da Indução Completa	78
5.6.1	Formulação do PIC usando conjuntos	79
5.7	Exercícios	80
5.8	Princípio da Boa Ordenação	80
5.9	Formas equivalentes do princípio da indução	81
5.9.1	PIM implica PBO	81
5.9.2	PBO implica PIC	82
5.9.3	PIC implica PIM	82
5.10	Exercícios adicionais	83
6	Relações	85
6.1	Conceitos básicos	85
6.1.1	Domínio e imagem	86
6.1.2	Restrição de relações	87
6.1.3	Relações de identidade	87
6.1.4	Relação inversa	87
6.1.5	Imagem e imagem inversa de conjuntos	88
6.2	Composição de relações	88
6.2.1	Notação alternativa	89
6.2.2	Composição com identidade	89
6.2.3	Composição com a relação inversa	89
6.2.4	Inversa da composição	90
6.2.5	Composição e inclusão	90
6.2.6	Potências de uma relação	90
6.3	Representação de relações usando matrizes	91
6.3.1	Matriz booleana de uma relação	91
6.3.2	Operações com relações usando matrizes	92
6.4	Tipos de relações	93
6.4.1	Composição e transitividade	94

6.4.2	Propriedades de relações usando matrizes	95
6.5	Fechos de uma relação	96
6.5.1	Fecho reflexivo	96
6.5.2	Fecho simétrico	97
6.5.3	Fecho transitivo	97
6.5.4	Fecho em geral	99
6.6	Relações de ordem	100
6.6.1	Diagrama de Hasse	102
6.6.2	Relações de ordem estrita	103
6.6.3	Ordem total	103
6.6.4	Ordem lexicográfica	104
6.6.5	Ordens “parciais”	105
6.6.6	Elementos mínimos e máximos	105
6.6.7	Elementos minimais e maximais	106
6.7	Relações de equivalência	108
6.7.1	Classes de equivalência	109
6.7.2	Relações de equivalência e partições	110
7	Funções, sequências e relações n-árias	113
7.1	Funções	113
7.1.1	Conceito	113
7.1.2	Domínio e imagem de uma função	114
7.1.3	As funções piso e teto	114
7.1.4	Função injetora, sobrejetora e bijetora	115
7.1.5	Composição de funções	116
7.1.6	Função inversa	117
7.1.7	Imagem e imagem inversa de conjuntos	118
7.1.8	Restrição de funções	118
7.1.9	Permutações	119
7.1.10	Funções idempotentes	120
7.2	Sequências finitas	120
7.2.1	Notação para sequências finitas	120
7.2.2	Índice inicial padrão	120
7.2.3	Comprimento	121
7.2.4	Concatenação	121
7.2.5	Subsequências e subcadeias	122
7.2.6	n -uplas	122
7.3	Produto cartesiano de n conjuntos	122
7.4	Relações n -árias	122
7.4.1	Definição	122
7.4.2	Projeção	123
7.4.3	Permutação de componentes	124
7.4.4	Restrição	124
7.4.5	Junção	124

8 Somatórias e produtórias	127
8.1 Introdução	127
8.2 Somatórias básicas	128
8.3 Manipulação de somatórias	128
8.4 Somatórias múltiplas	132
8.4.1 Mudança de ordem de somatórias	132
8.4.2 Distributividade generalizada	133
8.5 Majoração de somatórias	134
8.5.1 Majoração dos termos	134
8.5.2 Majoração por indução matemática	134
8.5.3 Majoração por integrais	136
8.6 Somas infinitas	139
8.7 Produtórias	140
8.8 Iteração de outras operações	142
9 Sequências infinitas e recorrências	143
9.1 Sequências infinitas	143
9.2 Especificando sequências infinitas	143
9.3 Recorrência	144
9.4 Resolução de recorrências	145
9.4.1 Recorrência aditiva simples	145
9.4.2 Recorrência multiplicativa simples	146
9.4.3 Recorrências lineares homogêneas	146
9.5 Recorrências lineares não homogêneas	148
9.6 Majoração e minoração de recorrências	149
10 Contagem	151
10.1 Permutações	151
10.1.1 Fórmula de Stirling	152
10.2 Arranjos	152
10.3 Combinações	153
10.3.1 Casos especiais	154
10.3.2 Propriedades	154
10.3.3 Fórmula do Binômio de Newton	155
10.3.4 Fórmula recursiva	156
10.4 Cardinalidade da união de conjuntos	156
10.5 Combinações múltiplas	157
11 Cardinalidade de conjuntos	161
11.1 Conjuntos finitos	161
11.2 Conjuntos infinitos	161
11.3 Conjuntos enumeráveis e contáveis	163
11.4 Comparação de cardinalidades	164
11.4.1 Teorema de Cantor	164
11.4.2 Cardinalidades de Cantor	165

12	Introdução à Teoria de Grafos	167
12.1	Introdução	167
12.2	Variedades de grafos	168
12.2.1	Grafos orientados e não orientados	169
12.2.2	Arestas paralelas	169
12.2.3	Laços	169
12.2.4	Grafos simples e multigrafos	169
12.2.5	Grafos finitos e infinitos	169
12.3	Definições formais	170
12.3.1	Arestas como pares ordenados	170
12.3.2	Arestas como pares não ordenados	170
12.3.3	Arestas como objetos com origem e destino	171
12.3.4	Arestas como objetos com dois extremos	172
12.3.5	Convenções para este livro	172
12.4	Conceitos fundamentais	173
12.4.1	Grafo vazio e sem arestas	173
12.4.2	Incidência	173
12.4.3	Adjacência	173
12.4.4	Grau do vértice	173
12.4.5	Grafos regulares	174
12.4.6	Grafos completos	175
12.5	Percursos em grafos	175
12.5.1	Passeios, trilhas e caminhos	175
12.5.2	Inversão e concatenação e de passeios	176
12.5.3	Circuitos e ciclos	177
12.5.4	Passeios orientados	177
12.6	Subgrafos	178
12.6.1	União e intersecção de subgrafos	179
12.6.2	Grafos complementares	180
12.7	Representação matricial de grafos	180
12.7.1	Matriz de adjacência	180
12.7.2	Matriz de incidência	181
12.8	Isomorfismos de grafos	181
12.8.1	Contagem de grafos	184
12.9	Conexidade	184
12.9.1	Conexidade em grafos não orientados	184
12.9.2	Conexidade em grafos orientados	185
12.10	Árvores	186
12.11	Grafos bipartidos	187
12.12	Grafos eulerianos	188
12.13	Grafos hamiltonianos	189
12.14	Grafos planares	192
12.14.1	A fórmula de Euler para grafos planares	194
12.14.2	O teorema de Kuratowski	195
12.14.3	Grafo dual	197

12.15	Coloração de grafos	197
12.15.1	Coloração de mapas	197
12.15.2	Coloração de grafos em geral	198
13	Probabilidade	201
13.1	Definição	202
13.1.1	Distribuição uniforme	202
13.1.2	Princípio da exclusão mútua	203
13.1.3	Princípio da exaustão	203
13.1.4	Princípio da complementaridade	203
13.1.5	Princípio da exclusão e inclusão	204
13.1.6	Princípio da independência	204
13.1.7	Relação com a lógica clássica	205
13.2	Variável aleatória	205
13.3	Valor esperado	206
13.3.1	Propriedades do valor esperado	208
13.4	Mediana	208
13.5	Moda	209
13.6	Variância e desvio padrão	210
13.6.1	Propriedades da variância	211
13.6.2	Desvio padrão	211
13.6.3	Covariância	212
13.6.4	Coefficiente de correlação	212
13.7	Probabilidade condicional	213
13.8	Inferência bayesiana	214
13.9	Teoria da informação	216
13.9.1	Capacidade de informação	216
13.9.2	Quantidade de informação	218
13.9.3	Quantidade esperada de informação	218

Prefácio

Objetivos e escopo. Este livro pretende ser um texto introdutório a algumas áreas da matemática discreta que são de especial importância para cursos de computação, ao nível de graduação e de mestrado.

Excluimos do escopo deste livro os fundamentos da matemática do contínuo — cálculo diferencial e integral, equações diferenciais e integrais, álgebra linear, e geometria analítica — pois acreditamos que um bom currículo de computação deve cobrir esses assuntos através de várias disciplinas específicas, ainda nos primeiros anos de graduação. Pela mesma razão, excluimos cálculo numérico, e limitamos nossa exposição de probabilidade e estatística aos conceitos fundamentais. Ainda pela mesma razão, evitamos completamente a área de algoritmos, computabilidade e complexidade, bem como assuntos específicos (e quase obrigatórios) de currículos de computação, como programação inteira, autômatos e linguagens formais.

Na verdade, cada um dos capítulos deste livro poderia ser coberto por uma disciplina separada do currículo de computação. Este livro deve ser visto, em primeiro lugar, como um “curso de alfabetização”, que procura ensinar as definições e conceitos essenciais para comunicação técnica em teoria da computação.

Para atingir esse objetivo, tivemos que sacrificar a profundidade pela abrangência. Em um livro ou artigo sobre um assunto específico, é normal o autor escolher um conjunto de definições e notações, e usá-las consistentemente na obra toda, ignorando as outras escolhas possíveis. Mas esta atitude não seria adequada para este livro. Assim, por exemplo, dedicamos um bom espaço às múltiplas definições incompatíveis de conceitos fundamentais, como “número natural” (inclui ou não o zero?), “função”, “grafo”, e muitas outras, e às variações de notação que os estudantes podem vir a encontrar na literatura. Só depois dessas discussões é que adotamos uma definição ou notação específica, para uso no resto do livro.

Por outro lado, não nos preocupamos em enunciar, muito menos provar, os teoremas que são considerados fundamentais dessas áreas — exceto a título de exemplo de uso dos conceitos. Assim, nosso tratamento de grafos (capítulo 12) não pretende substituir disciplinas de teoria dos grafos, onde esses resultados devem ser cobertos em detalhe. Seu objetivo é apenas dar ao estudante familiaridade com os conceitos e vocabulário da área — para facilitar seu acompanhamento dessas disciplinas, e para que ele consiga entender e usar a linguagem de grafos em outras áreas da computação. O mesmo vale para todos os outros capítulos.

Lógica matemática. Professores de disciplinas computação com conteúdo teórico frequentemente observam a grande dificuldade que seus alunos tem em formalizar seu raciocínio. A raiz desse problema é a dificuldade que muitos alunos tem em perceber a diferença entre uma prova rigorosa e uma coleção de frases aleatórias e inconclusivas, mesmo que com vocabulário ma-

temático, que termina com a conclusão esperada.

Acontece que essa não é uma habilidade nata. Seu apredizado requer, além de anos de prática, o conhecimento dos fundamentos da lógica. Embora as demonstrações que se encontram na literatura (e que os professores esperam que os alunos produzam) quase nunca sejam *formais* — sequências de fórmulas lógicas, encadeadas por aplicações de regras de inferência — o que caracteriza uma prova rigorosa é o fato de que ela pode ser *formalizada*. Assim, a lógica é o esqueleto *invisível* que sustenta e caracteriza uma demonstração válida.

Por esse motivo, optamos por iniciar nosso livro com uma exposição da lógica matemática, nas suas duas formulações clássicas — a teoria de conjuntos, por um lado, e a lógica proposicional e cálculo de predicados, pelo outro. Estamos supondo que os leitores deste livro já tiveram contato com o conceito de conjuntos, graças a disciplinas de matemática anteriores; portanto não julgamos necessário dedicar mais que algumas páginas a esse assunto. Por outro lado, acreditamos que poucos leitores possuem conhecimento do cálculo de proposições e predicados (apesar do uso de operações booleanas em programação). Além disso, com a eliminação da geometria euclidiana dos currículos de ensino médio, os estudantes que ingressam na universidade dificilmente tiveram contato com os conceitos de axiomas, teoremas, e demonstrações formais. Por essa razão, dedicamos três capítulos inteiros (3, 4 e 5) a esses tópicos — sendo que o último é inteiramente dedicado a técnicas de prova por indução.

Relações e funções. Outro tópico ao qual resolvemos dedicar bastante espaço é o conceito de relação. Relações são muito usadas em todas as áreas teóricas e práticas da computação, incluindo autômatos e circuitos lógicos, estruturas e bancos de dados, redes e comunicações digitais, etc..

Na literatura há duas principais abordagens para este conceito. Segundo uma abordagem, uma relação entre dois conjuntos é uma tripla (A, B, R) onde A e B são conjuntos, e R é um subconjunto do produto cartesiano $A \times B$. Na outra abordagem, uma relação entre A e B é apenas um subconjunto de $A \times B$. Esta diferença tem inúmeras repercussões em conceitos derivados, e inclusive na linguagem. Por exemplo, na primeira abordagem a relação tem um domínio “nominal” (A), que é distinto de seu domínio “efetivo” (os elementos de A que aparecem no lado esquerdo de pares de R). Na segunda abordagem, pelo contrário, existe apenas o domínio efetivo. A mesma observação vale para o contra-domínio. Na primeira abordagem existem infinitas relações vazias (com $R = \emptyset$), enquanto que na segunda só existe uma. Na primeira abordagem podemos dizer que uma relação é sobrejetora ou bijetora, enquanto que na segunda temos que especificar os conjuntos e dizer “sobrejetora em B ” e “bijetora entre A e B ”.

Cada abordagem tem suas vantagens e desvantagens. Constatamos inclusive que muitos livros textos são inconsistentes neste ponto, e adotam ora uma definição, ora outra, conforme as conveniências do momento. Debates muito qual destas duas abordagens deveríamos adotar para os capítulos seguintes (veja a figura ??), e por fim resolvemos adotar a segunda (conjunto de pares, sem domínio e contra-domínio).

Enfrentamos um dilema semelhante na seção sobre relações de ordem, pois para esse conceito também há várias escolhas incompatíveis (ou mesmo ilógicas) de nomenclatura. Por exemplo, os termos “ordem parcial” e “ordem total” não são mutuamente exclusivos (como se esperaria pelo dicionário), mas um inclui o outro. E “relação de ordem estrita” não é um caso particular de relação de ordem, mas um conceito praticamente disjunto (uma é reflexiva e a outra é irreflexiva). Além disso, os termos “elemento mínimo” e “elemento máximo” são enganosos quando são aplicados

à relação “ \geq ” (ou a outras relações sobre números que não “ \leq ”). Mas não cabe a este livro propor nomenclaturas mais consistentes; tudo o que podemos fazer é alertar o estudante para essas armadilhas.

Somatórias e produtórias. Dentro dos objetivos deste livro, nosso tratamento de somatórias e produtórias (capítulo 8) dá mais ênfase à “linguagem” do que a resultados avançados da teoria. Assim, tomamos cuidado de expor o leitor às várias convenções da notação, e procuramos ensinar as principais técnicas de manipulação de somatórias (como troca de índices e mudança de ordem de soma). Por outro lado, também procuramos desenvolver a intuição dos estudantes, apontando as analogias entre somatórias e integrais (que eles supostamente conhecem de cálculos anteriores).

Sequências e recorrências. Procuramos seguir a mesma filosofia no capítulo 9, que trata de sequências definidas por recorrências. Além de apresentar a linguagem, enfatizamos a técnica geral de resolução para recorrências lineares homogêneas, que resolve muitos dos problemas encontrados em computação.

Contagem. A análise combinatória é fundamental tanto para a análise de algoritmos quanto para inúmeras áreas práticas, e deveria merecer uma disciplina à parte. Neste livro nos limitamos a rever os conceitos de permutações, arranjos e combinações, e o teorema da inclusão e exclusão. Embora esses assuntos sejam oficialmente vistos no segundo grau, consideramos oportuno rever as definições e fórmulas básicas, especialmente à luz dos conceitos de indução e recorrências vistos nos capítulos anteriores. Uma vez que problemas de contagem raramente admitem fórmulas simples e exatas, consideramos oportuno também apresentar a fórmula de aproximação de Stirling para a função fatorial.

Cardinalidade de conjuntos infinitos. A rigor, a teoria das cardinalidades infinitas tem pouca utilidade prática em computação. Porém, a distinção entre infinidades enumeráveis e não enumeráveis é relevante para a teoria da computação. Por exemplo, a existência de funções não computáveis decorre trivialmente da observação de que o conjunto de funções de \mathbb{N} para \mathbb{N} tem cardinalidade \aleph^1 , enquanto que o conjunto de todos os algoritmos tem cardinalidade \aleph^0 . Além disso, o argumento de diagonalização usado para provar que \mathbb{R} não é enumerável é usado, por exemplo, na demonstração do teorema de Turing.

Consideramos também que essa área é um capítulo importante da história da matemática, e portanto é “cultura geral” quase que obrigatória para quem tem curso superior em ciência ou tecnologia. Por outro lado, esse assunto nem sempre é visto nas outras disciplinas de matemática dos currículos de computação. Por essas razões, optamos por incluir um curto resumo desses conceitos neste livro (capítulo 11).

Probabilidade. Optamos por incluir neste livro um capítulo sobre noções elementares de estatística e probabilidade. Embora esses tópicos sejam frequentemente excluídos de currículos de computação, constatamos que eles são essenciais para várias disciplinas teóricas e aplicadas, como análise de algoritmos, criptografia, redes e serviços distribuídos, sistemas operacionais, compiladores, processamento de imagens, reconhecimento de padrões, e processamento de linguagens naturais. A teoria da probabilidade é também a fundação da teoria da informação (incluindo o

conceito de bit!) e portanto para a análise de sistemas de comunicação, digitais ou não. Além disso, a teoria da probabilidade é parte da evolução da lógica matemática, o passo seguinte após o desenvolvimento do cálculo de predicados.

Capítulo 1

Introdução à lógica matemática

1.1 Como ter certeza?

Você escreveu um programa, ou inventou um algoritmo, para resolver um certo problema. Como pode você se convencer que ele funciona? Como pode você convencer os outros que ele funciona?

Uma maneira de adquirir confiança sobre um algoritmo é testá-lo. Porém, para a maioria dos algoritmos, é impossível montar testes que verifiquem absolutamente todos os casos possíveis que podem ocorrer durante sua execução. Muitos programadores podem citar exemplos de programas que funcionaram perfeitamente em todos os testes, mas falharam imediatamente quando usados na prática.

1.2 A invenção da lógica

Essa questão — como ter certeza que nosso raciocínio é correto, e como transmitir aos outros essa certeza — foi estudada pelos gregos séculos antes de Cristo. Eles observaram que uma maneira de conseguir esse tipo de certeza, e para passar essa certeza a outras pessoas, é começar por um conjunto de *axiomas*, fatos simples que todos concordam que são verdade; e desenvolver um raciocínio a partir desses axiomas, usando *regras de inferência*, maneiras de raciocinar que todos concordam que são válidas. Com isso eles inventaram a *lógica*, que eles consideravam um ramo da *retórica*, a arte de discursar e convencer pessoas.

O filósofo grego Aristóteles (384–322 A.C.), em particular, estudou os chamados *silogismos*, raciocínios em que, partindo de duas premissas cuja verdade é aceita, obtém-se uma conclusão nova que é necessariamente verdadeira. Por exemplo, se acreditamos nas premissas “todos os homens são mortais” e “Sócrates é um homem”, então temos que acreditar também que “Sócrates é mortal.”. Ou então, se acreditamos que “nenhum mamífero tem penas”, e que “morcegos são mamíferos”, então temos que acreditar que “morcegos não tem penas”.

1.3 Euclides e demonstrações geométricas

Enquanto isso, os arquitetos e engenheiros gregos tinham preocupações semelhantes em relação aos “algoritmos geométricos” — construções com régua e compasso — que eles usavam em seus

projetos. Por exemplo, a receita da figura 1.1 supostamente constrói um pentágono com todos os lados e ângulos iguais.

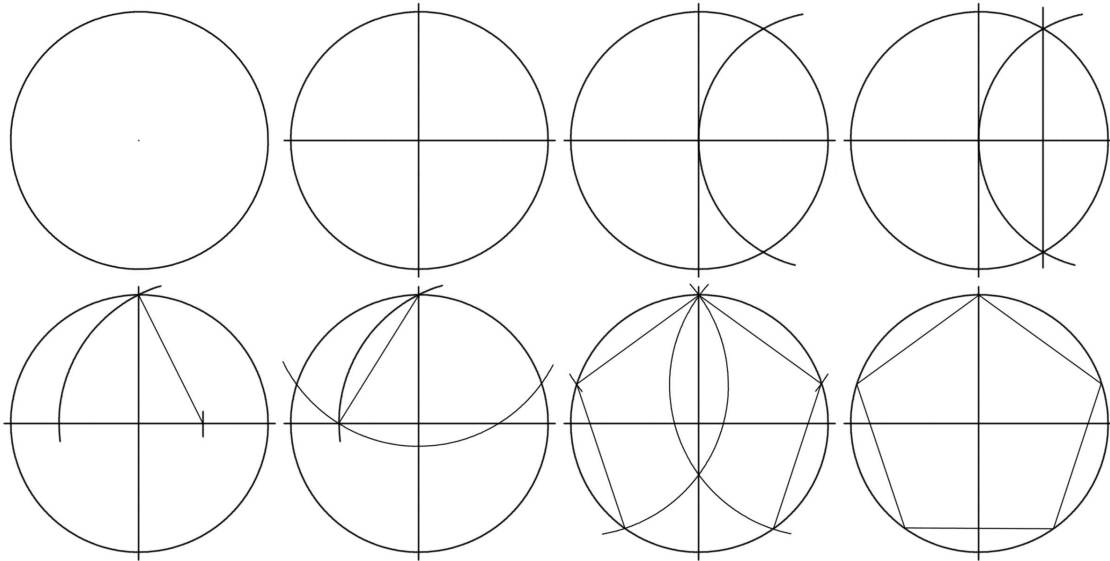


Figura 1.1: **Construção de um pentágono regular.**

Como podemos ter certeza de que essa construção realmente faz isso? Podemos efetuá-la numa folha de papel e medir os ângulos; mas tanto os passos da construção quanto a medida final tem sempre pequenos erros, e portanto esse teste não vai dizer se a construção é matematicamente correta ou apenas aproximada. Se as diferenças entre os ângulos são desprezíveis no papel, será que serão desprezíveis quando esse algoritmo for usado na construção de um anfiteatro?

O primeiro a descrever um sistema lógico completo para a geometria da época foi o geômetra grego Euclides (que viveu por volta do século III antes de Cristo), no seu livro *Elementos de Geometria* [9]. Euclides começou enumerando dez axiomas sobre conceitos geométricos (pontos, retas, círculos, distâncias, ângulos), como por exemplo

- *Por dois pontos distintos do plano passa uma única reta.*
- *Qualquer segmento de reta pode ser prolongado indefinidamente nos dois sentidos.*
- *É possível contruir um círculo com quaisquer centro e raio dados.*
- *Todos os ângulos retos são iguais.*

Em seguida Euclides mostrou centenas de outras afirmações (*teoremas*) que decorrem desses axiomas, como por exemplo

- *Se um triângulo tem os três lados iguais, ele tem os três ângulos iguais.*
- *Duas retas que são perpendiculares a uma terceira são paralelas entre si.*
- *Num triângulo retângulo, o quadrado do maior lado é a soma dos quadrados dos outros dois lados.*

Muitos desses teoremas são afirmações de que certas construções geométricas, como a da figura 1.1, produzem o resultado desejado. Principalmente, para cada teorema, ele também escreveu uma *prova* ou *demonstração* — uma sequência de passos lógicos que, começando com os axiomas e teoremas já provados, convence qualquer leitor de que o novo teorema é verdadeiro.

1.4 Álgebra

A lógica de Euclides e outros filósofos gregos foi extensamente usada por mais de dois mil anos. Entretanto, por muitos séculos o hábito de provar as afirmações foi limitado apenas à geometria. Embora os gregos conhecessem muitas propriedades de números (por exemplo, os conceitos de divisor comum e número primo), para demonstrar tais propriedades eles geralmente convertiam os números em comprimentos de retas, e usavam a linguagem da geometria. Esse é o caso, por exemplo, do *algoritmo de Euclides* para calcular o máximo divisor comum de dois números — que é considerado por muitos o mais antigo algoritmo não trivial. Na descrição original de Euclides, o problema é dividir dois segmentos de reta dados em partes iguais e de maior tamanho possível.

Na idade média, entretanto, o matemático árabe Al-Khowarizmi inventou a *álgebra*, outra maneira de provar afirmações sobre números e convencer pessoas de que uma dada sequência de operações aritméticas alcança o resultado desejado. Na álgebra, os números são representados abstratamente por letras, e as operações ou afirmações sobre esses números são indicadas com símbolos como ‘+’ ou ‘>’. A álgebra também fornece algumas fórmulas, como $A + B = B + A$ e $A \times (B + C) = (A \times B) + (A \times C)$, que representam afirmações que são sempre verdadeiras, quaisquer que sejam os números que vierem a substituir as variáveis. A álgebra também fornece certas regras fundamentais que permitem transformar uma fórmula em outra fórmula equivalente, ou combinar fórmulas corretas para produzir novas fórmulas corretas. Por exemplo, se sabemos que $A > B$ e $B > C$ podemos concluir com certeza que $A > C$.

1.5 As linguagens da lógica matemática

Como resultado desse desenvolvimento histórico, dispomos hoje de dois principais sistemas de notação, ou *linguagens formais*, para expressar raciocínios lógicos de maneira matematicamente clara, sucinta, e, principalmente, livre de ambiguidades. Estas linguagens são a *teoria de conjuntos* e o *cálculo de predicados*.

A lógica clássica somente lida com afirmações que são verdadeiras ou falsas. Essa característica praticamente restringe o uso da lógica para afirmações matemáticas. Mas no século 16 e 17 matemáticos começaram a estudar o cálculo de chances em jogos de azar (dados, roletas, loteria, etc.). No início do século 20 estas investigações haviam evoluído para a *teoria da probabilidade*, que permite expressar nosso grau de confiança a respeito de afirmações incertas, e raciocinar com precisão sobre elas; e para a *estatística*, um conjunto de técnicas para analisar dados experimentais que supostamente confirmam ou refutam tais afirmações.

Em meados do século XX, motivada pela expansão do rádio, telefone e outros meios eletrônicos de comunicação, a teoria da probabilidade por sua vez deu origem à *teoria da informação*, que permite determinar, por exemplo, a capacidade real de canais de comunicação na presença de distúrbios aleatórios no sinal recebido. Finalmente, com o surgimento do computador digital, sur-

giram disciplinas matemáticas específicas para raciocinar precisamente com programas e estruturas de dados, incluindo *análise de algoritmos*, *teoria da computabilidade e complexidade de funções*, *criptografia digital*, e muitas outras.

Capítulo 2

Teoria dos Conjuntos

Acreditamos que o leitor já teve contato com os conceitos básicos da teoria dos conjuntos, como *elemento*, *união*, *intersecção*, etc.. Nesta seção vamos revisar esses conceitos.

Embora seja possível desenvolver a teoria de conjuntos de maneira axiomática, como foi feito por Georg Cantor (1845–1918) e Ernest Zermelo (1871–1953), a abordagem informal apresentada é suficiente para nossos propósitos.

Um *conjunto* é um conceito primitivo, que informalmente pode ser entendido como uma coleção *não ordenada* de entidades distintas, chamadas de *elementos* do conjunto.

Dizemos que um elemento x *pertence* a um conjunto A se x é um elemento de A . Denotamos este fato por $x \in A$. Para denotar que x *não pertence* a A , ou seja, que x não é um elemento do conjunto A , escrevemos $x \notin A$.

Se x pertence a um conjunto A , diz-se também que A *tem* (ou *possui*) x , e escreve-se $A \ni x$. A negação desta afirmação (A *não tem* ou *não possui* x) é denotada por $A \not\ni x$. Não é correto dizer que A “contém” x , pois este termo é usado em matemática com um sentido bem diferente (veja a seção 2.4)

2.1 Especificando conjuntos

Podemos especificar um conjunto de diversas formas. Se um conjunto tem poucos elementos, podemos listá-los, um a um, em qualquer ordem, entre chaves ‘{}’. Por exemplo, o conjunto cujos elementos são os números inteiros 2, 3 e 5 pode ser escrito $\{2, 3, 5\}$. Assim, por exemplo, temos que $3 \in \{2, 3, 5\}$, mas $4 \notin \{2, 3, 5\}$.

Outra maneira de especificar um conjunto através das propriedades de seus elementos. Para tanto, usamos a notação $\{a : P(a)\}$, onde a é uma variável arbitrária e $P(a)$ uma afirmação matemática que pode ser verdadeira ou falsa dependendo do valor de a . Por exemplo,

$$\{a : a \text{ é um número inteiro e } -5 < a < 5\}$$

é outra maneira de definir o conjunto $\{-4, -3, -2, -1, 0, +1, +2, +3, +4\}$.

Exercício 2.1: Escreva explicitamente os elementos dos seguintes conjuntos:

1. $A = \{x : x \in \mathbb{Z} \text{ e } x^2 - 2x + 1 \leq 0\}$.
2. $A = \{x : x \in \mathbb{Z}, 2 \leq x \leq 20 \text{ e } x \text{ é primo}\}$.

$$3. A = \{x : x \in \mathbb{R} \text{ e } x^2 - 2x = 0\}.$$

Existem alguns conjuntos de números que são muito usados em matemática, e tem notações convencionais bem estabelecidas:

- o conjunto dos *números inteiros* \mathbb{Z} ,
- o conjunto dos *números naturais* $\mathbb{N} = \{x : x \in \mathbb{Z} \text{ e } x \geq 0\}$,
- o conjunto dos *números racionais* $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ e } b \neq 0\right\}$, e
- o conjunto dos *números reais* \mathbb{R} .

2.1.1 Definições circulares e contraditórias

A definição de um conjunto pode usar outros conjuntos, como por exemplo “seja X o conjunto de todos os elementos que estão no conjunto Y mas não no conjunto Z ”. Porém, deve-se tomar cuidado para evitar definições circulares, que podem não ter sentido. Um exemplo clássico é a definição “seja X o conjunto de todos os elementos que não pertencem a X ”. Esta “definição” não faz sentido pois diz que um elemento que está em X não está em X , e vice-versa.

Este contra-exemplo teve um papel muito importante no desenvolvimento da teoria de conjuntos. Ele é conhecido pelo nome *Paradoxo de Russel*, por ter sido observado pelo matemático inglês Bertrand Russel (1872–1970). Ele é conhecido também como *Paradoxo do Barbeiro*, pois foi exemplificado com uma anedota em que o barbeiro de um quartel recebeu a ordem de fazer a barba de todos os que não fizessem sua própria barba, e apenas esses — deixando o barbeiro na dúvida sobre o que ele deveria fazer com a sua.

Por outro lado, há definições circulares de conjuntos que são perfeitamente válidas. Por exemplo, considere o conjunto de inteiros X que contém o inteiro 1, não contém o inteiro 0, contém $x + 2$ e $x - 2$ qualquer que seja o elemento x de X . Pode-se verificar que o único conjunto X com estas propriedades é o conjunto dos inteiros ímpares. Para entender porque esta definição é válida vamos precisar do conceito de indução matemática, que será visto no capítulo 5.

2.2 Igualdade de conjuntos

Por definição, um conjunto A é igual a um conjunto B se, e somente se, todo elemento de A é elemento de B , e todo elemento de B é elemento de A . Esta condição, denotada por $A = B$, significa que A, B são o mesmo conjunto.

Dito de outra forma, dois conjuntos A e B são diferentes ($A \neq B$) se, e somente se, existe um elemento de A que não pertence a B , ou um elemento de B que não pertence a A .

Observe que, como os conjuntos não são ordenados, o conjunto $\{1, 2, 3\}$ é igual ao conjunto $\{3, 2, 1\}$.

2.3 Conjunto vazio

É possível definir conjuntos sem elementos. Dizemos que tal conjunto é *vazio*. Por exemplo, considere o conjunto $A = \{x : x \in \mathbb{R} \text{ e } x = x + 1\}$. Pela regra da seção 2.2, todos os conjuntos vazios são iguais; ou seja existe um único conjunto vazio, que é geralmente denotado por \emptyset .

2.4 Relação de inclusão

Sejam A e B dois conjuntos. Dizemos que A é um *subconjunto* de B se, e somente se, todo elemento de A é um elemento de B . Neste caso, dizemos também que A *está contido em* B , ou que B *contém* A . Denotamos esta condição por $A \subseteq B$ ou $B \supseteq A$.

Se existe um elemento de A que não pertence a B , então A não é subconjunto de B , e escrevemos $A \not\subseteq B$. De acordo com esta definição, todo conjunto está contido em si próprio e contém o conjunto vazio; ou seja, $A \subseteq A$ e $\emptyset \subseteq A$, para qualquer conjunto A .

Se $A \subseteq B$ mas $A \neq B$, dizemos que A é um sub-conjunto *próprio* de B , que denotamos por $A \subset B$ ou $B \supset A$. Analogamente, $A \not\subset B$ significa que A não é um subconjunto próprio de B .

2.5 Cardinalidade

Informalmente, dizemos que um conjunto A é *finito* se ele tem um número finito $n \in \mathbb{N}$ de elementos. Este número é a *cardinalidade* de A , denotada por $|A|$ ou $\#A$. Observe que $|A| = 0$ se e somente se $A = \emptyset$.

Dizemos que um conjunto é *infinito* se ele não é finito. Os conjuntos \mathbb{N} , \mathbb{Z} , \mathbb{Q} , e \mathbb{R} são infinitos.

Conjuntos infinitos não podem ter seus elementos listados explicitamente. Informalmente, é comum usar ‘...’ nesses casos, por exemplo

- $\mathbb{N} = \{0, 1, 2, \dots\}$
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, +1, +2, +3, \dots\}$

Entretanto, esta notação deve ser evitada pois pode ser ambígua. Por exemplo, o que é o conjunto $\{2, 3, 5, 7, \dots\}$?

2.6 Operações com conjuntos

Para os próximos conceitos sejam A e B dois conjuntos.

2.6.1 União e intersecção

A *união* de A e B , denotada por $A \cup B$, é o conjunto de todos os elementos que estão em pelo menos um dos conjuntos, A ou B .

Exemplo 2.1: Se $A = \{1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$ então $A \cup B = \{1, 2, 3, 4, 5\}$.

A *intersecção* de A e B , denotada por $A \cap B$, é o conjunto de todos os elementos que estão em ambos os conjuntos, A e B .

Exemplo 2.2: Se $A = \{1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$ então $A \cap B = \{2, 3\}$.

Se $A \cap B = \emptyset$ dizemos que os conjuntos A e B são *disjuntos*.

2.6.2 Diferença, universo, e complemento

A *diferença de A e B* é o conjunto de todos os elementos de A que não estão em B . Este conjunto é também chamado *A menos B* , ou o *complemento de B em A* , e é denotado por $A - B$ ou $A \setminus B$.

Em certos casos, é conveniente supor que todos os elementos de todos os conjuntos que nos interessam pertencem a um *conjunto universal* ou *universo*, que denotaremos por \mathcal{U} . Se A é o conjunto universo \mathcal{U} , então $\mathcal{U} - B$ é chamado o *complemento de B* e denotado por \bar{B} ou B^c .

Observe que se $A \subseteq B$ então $A \cup B = B$, $A \cap B = A$ e $\bar{B} \subseteq \bar{A}$.

Exercício 2.2: Dê exemplos em que $(A \cup B) - B = A$ e $(A \cup B) - B \neq A$

Exercício 2.3: Sejam $\mathbb{U} = \{n \in \mathbb{N} : 0 \leq n \leq 9\}$, $A = \{1, 2, 3, 4\}$, $B = \{x \in \mathbb{R} : (x-1)(x-3)^3 = 0\}$ e $C = \{n \in \mathbb{N} : n \text{ é ímpar}\}$. Calcule:

1. $A \cup B$.
2. $A \cap (B \cup C)$.
3. $C - A$.
4. A cardinalidade de A , B e C .
5. $\bar{A} \cup C$.

Exercício 2.4: Sejam A e B dois conjuntos finitos quaisquer. Encontre uma fórmula matemática que relaciona $|A|$, $|B|$, $|A \cap B|$ e $|A \cup B|$.

2.6.3 Diferença simétrica

Outra operação de conjuntos é a *diferença simétrica*, denotada por $A \oplus B$ ou $A \Delta B$, que consiste de todos os elementos que estão em *exatamente* um dos dois conjuntos. Isto é,

$$A \Delta B = (A \setminus B) \cup (B \setminus A) \tag{2.1}$$

A figura 2.1 mostra uma representação gráfica das operações de conjuntos:

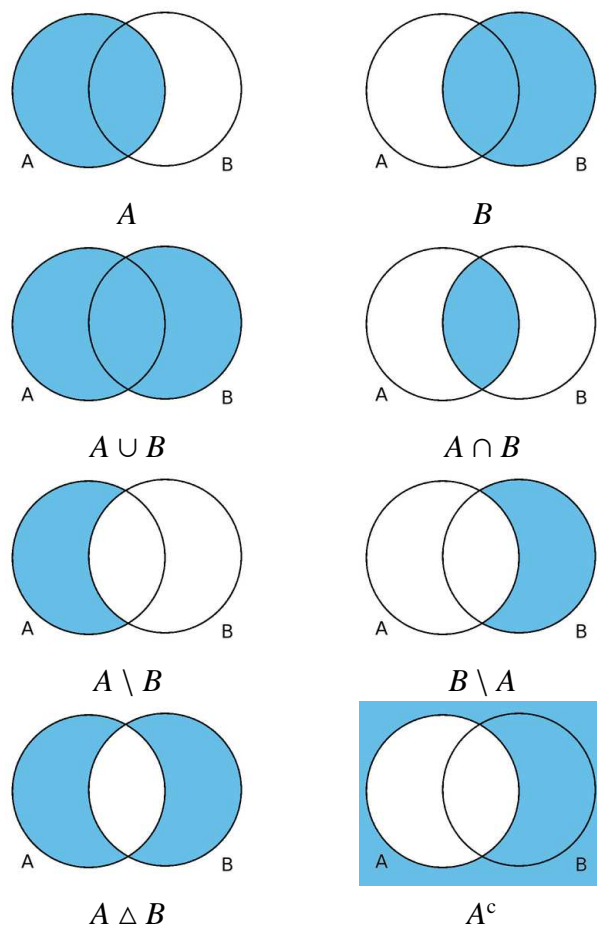


Figura 2.1: Operações com conjuntos.

Esta representação gráfica para conjuntos é chamada de *diagrama de Venn*, por ter sido introduzida pelo matemático inglês John Venn (1834–1923).

2.6.4 Propriedades das operações com conjuntos

A seguir listaremos algumas propriedades que são satisfeitas pelas operações com conjuntos.

- *Propriedades da comutatividade*

- $A \cup B = B \cup A$.

- $A \cap B = B \cap A$.

- *Propriedades da associatividade*

- $A \cup (B \cup C) = (A \cup B) \cup C$.

- $A \cap (B \cap C) = (A \cap B) \cap C$.

- *Propriedades da distributividade*

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

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

- *Propriedades da idempotência*

$$- A \cup A = A.$$

$$- A \cap A = A.$$

- *Leis de De Morgan*

$$- \overline{A \cup B} = \bar{A} \cap \bar{B}.$$

$$- \overline{A \cap B} = \bar{A} \cup \bar{B}.$$

Estas leis levam o nome do matemático inglês Augustus de Morgan (1806–1871), mas eram conhecidas desde a antiguidade.

- *Propriedades do complemento*

$$- \bar{\bar{A}} = A.$$

$$- A \cup \bar{A} = \mathcal{U}.$$

$$- A \cap \bar{A} = \emptyset.$$

$$- \bar{\mathcal{U}} = \emptyset.$$

$$- \bar{\emptyset} = \mathcal{U}.$$

- *Propriedades do conjunto universal*

$$- A \cup \mathcal{U} = \mathcal{U}.$$

$$- A \cap \mathcal{U} = A.$$

- *Propriedades do conjunto vazio*

$$- A \cup \emptyset = A.$$

$$- A \cap \emptyset = \emptyset.$$

Exercício 2.5: Usando diagramas de Venn, verifique que a diferença simétrica também é uma operação associativa e comutativa; isto é, que $A \triangle B = B \triangle A$ e $(A \triangle B) \triangle C = A \triangle (B \triangle C)$, para quaisquer conjuntos A , B e C .

2.7 Conjuntos de conjuntos

Conjuntos podem ser elementos de outros conjuntos. Por exemplo, o conjunto

$$A = \{\emptyset, \{2, 3\}, \{2, 4\}, \{2, 4, 7\}\}$$

é um conjunto com quatro elementos. Se B é o conjunto $\{2, 3\}$, temos que B é elemento de A ($B \in A$), mas B não é sub-conjunto de A ($B \not\subseteq A$). Note que \emptyset é elemento de A e também subconjunto de A , enquanto que $\{2\}$ não é nem uma coisa nem outra.

Em particular, o conjunto $A = \{\emptyset\}$ não é vazio, pois ele tem um elemento — o conjunto vazio. Observe que $|A| = 1$, enquanto que $|\emptyset| = 0$.

2.8 Conjunto potência

O conjunto de todos os subconjuntos de um conjunto A é chamado de *conjunto potência* de A , e denotado por $\mathbb{P}(A)$.

Exemplo 2.3: Se $A = \{1, 2, 3\}$ então $\mathbb{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Observe que se $A = \emptyset$ então $\mathbb{P}(A) = \{\emptyset\}$, e se $A = \{\emptyset\}$ então $\mathbb{P}(A) = \{\emptyset, \{\emptyset\}\}$.

Se A é um conjunto finito, então $|\mathbb{P}(A)| = 2^{|A|}$. Este fato será demonstrado no capítulo 5. Por esta razão, muitos autores denotam o conjunto potência de A por 2^A .

2.9 Partição

Seja A um conjunto, e P um conjunto cujos elementos são sub-conjuntos de A (isto é, $P \subseteq \mathbb{P}(A)$). Dizemos que P é uma *partição* de A se os elementos de P são não vazios, disjuntos dois a dois, e a união de todos os elementos de P é A . Nesse caso, cada elemento de P é também chamado de uma *parte* ou *bloco* da partição.

Exemplo 2.4: Se $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, o conjunto

$$P = \{\{1, 2, 5, 6, 7\}, \{3\}, \{4, 8, 10\}, \{9\}\}$$

é uma partição de A .

Observe que, para qualquer conjunto A , o conjunto $\{A\}$ é sempre uma partição de A . Além disso, se B é qualquer subconjunto próprio e não vazio de A ($\emptyset \subset B \subset A$), então o conjunto $\{B, A \setminus B\}$ também é uma partição de A .

O conjunto vazio tem apenas uma partição, que é o próprio conjunto vazio (sem nenhuma parte).

2.10 Produto cartesiano de dois conjuntos

2.10.1 Produto de dois conjuntos

Indicamos por (a, b) um *par ordenado* de elementos, no qual a é o *primeiro elemento* e b é o *segundo elemento*. Um par ordenado não deve ser confundido com um conjunto de dois elementos, pois a ordem é importante (por exemplo, o par $(10, 20)$ é diferente do par $(20, 10)$) e os dois elementos podem ser iguais (como por exemplo no par $(10, 10)$). Dois pares ordenados (a, b) e (c, d) são iguais (são o mesmo par) se, e somente se, $a = c$ e $b = d$.

Sejam A e B dois conjuntos. O *produto cartesiano*, denotado por $A \times B$, é o conjunto de todos os pares ordenados (a, b) com $a \in A$ e $b \in B$. Como no produto cartesiano os pares são ordenados, temos que $A \times B \neq B \times A$ (exceto quando $A = B$ ou $A = \emptyset$ ou $B = \emptyset$).

2.11 Exercícios

Exercício 2.6: Seja \mathbb{R} , o conjunto dos números reais. Considere os seguintes subconjuntos de \mathbb{R} :

- $(a, b) = \{x : a < x < b\}$ (*intervalo aberto*);
- $[a, b] = \{x : a \leq x \leq b\}$ (*intervalo fechado*);
- $(a, b] = \{x : a < x \leq b\}$ (*intervalo fechado à direita*),
- $[a, b) = \{x : a \leq x < b\}$ (*intervalo fechado à esquerda*),
- $(-\infty, a) = \{x : x < a\}$,
- $(-\infty, a] = \{x : x \leq a\}$,
- $(a, \infty) = \{x : a < x\}$,
- $[a, \infty) = \{x : a \leq x\}$,
- $(-\infty, \infty) = \mathbb{R}$,

Calcule

1. $[1, 3] \cap (2, 4)$.
2. $(-\infty, 2) \cap [-1, 0]$.
3. $(-\infty, 2) \cap [-1, 3]$.
4. $[0, 10] \cup [1, 11]$.
5. $(0, \infty) \cap (-\infty, 1)$.
6. $[-3, 0] \cup (0, 3]$.
7. $\overline{(0, 5]}$.

Exercício 2.7: Diagramas de Venn podem ser usados para três ou mais conjuntos. Um diagrama de Venn para três conjuntos A , B e C , por exemplo, precisa dividir o plano em 8 regiões, correspondendo a todas as possíveis relações (pertence ou não pertence) entre um elemento e esses três conjuntos. Desenhe tal diagrama e use-o para mostrar as seguintes fórmulas:

1. $A \cap B \cap C$.
2. $A \cup B \cup C$.
3. $(A \cup B) - C$.
4. $(A - B) \cup (B - C) \cup (C - A)$.

Exercício 2.8: Use diagramas de Venn para verificar as seguintes identidades:

1. $A - (A \cap B) = A - B$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
3. $(A \cup B) - C = (A - C) \cup (B - C)$.
4. $A \cup (B - C) = (A \cup B) - (C - A)$.

Exercício 2.9: Sejam A , B e C três conjuntos finitos quaisquer. Encontre uma fórmula matemática para $|A \cup B \cup C|$ em função de $|A|$, $|B|$, $|C|$, $|A \cap B|$, $|A \cap C|$, $|B \cap C|$ e $|A \cap B \cap C|$.

Capítulo 3

Lógica matemática

3.1 Lógica proposicional

3.1.1 Proposições e valores lógicos

Uma *proposição* é uma sentença declarativa que ou é verdadeira ou é falsa. Exemplos:

1. *O morcego é um mamífero.*
2. *Rio de Janeiro é a capital do Brasil.*
3. *Há 36 macacos no zoológico de Londres.*
4. *A taxa de juros do Banco Central vai subir amanhã.*
5. *O trilionésimo algarismo decimal de π é 7.*

Observe que não é necessário que saibamos se a sentença é verdadeira ou falsa. Este fato pode depender de informações que não temos no momento (como no exemplo 3 acima), de eventos que ainda não aconteceram (como no exemplo 4), ou de cálculos que não temos recursos para realizar (como no exemplo 5).

Como exemplos de frases que *não* são proposições, podemos citar

1. frases interrogativas, como “*O que é isto?*”,
2. frases imperativas, como “*Leia com cuidado*”,
3. certas sentenças auto referentes, como “*Esta frase é falsa*”.

Uma sentença declarativa que depende de variáveis pode ser considerada uma proposição em um contexto onde as variáveis tem valor determinado. Por exemplo, a sentença “*x é menor que 3*” isoladamente não é uma proposição. Porém, uma vez que o valor de x for definido, ela se torna uma proposição. Este ponto será tratado com mais detalhe na seção 3.6.

Dizemos que o *valor lógico* ou *valor-verdade* de uma proposição é *verdadeiro* se ela for verdadeira, e *falso* caso contrário.

3.1.2 Conectivos lógicos e proposições compostas

Todas as línguas naturais possuem *conectivos lógicos*, como “e”, “ou”, “não”, “se ... então”, que permitem combinar proposições simples para formar proposições mais complexas. Por exemplo,

1. [Brasília é a capital do Brasil,] e [Montevidéu é a capital da Argentina].
2. [Brasília é a capital do Brasil,] ou [Montevidéu é a capital da Argentina].
3. Se [a taxa de juros cair amanhã], então [a inflação vai aumentar neste mes].
4. Não [haverá sessão da meia-noite hoje neste cinema].

Uma proposição que não pode ser decomposta em proposições menores ligadas por conectivos lógicos é dita uma *proposição simples* ou *atômica*. Nos exemplos acima, os colchetes “[]” indicam as proposições simples.

O valor lógico (*verdadeiro* ou *falso*) de uma proposição deste tipo depende do valor lógico das proposições simples que a compõem, e da maneira como elas são combinadas pelos conectivos. Assim, se sabemos que a proposição “Brasília é a capital do Brasil” é verdadeira, e “Montevidéu é a capital da Argentina” é falsa, podemos concluir que a proposição 1 acima é falsa, mas a proposição 2 é verdadeira.

3.1.3 Notação para cálculo proposicional

A *lógica proposicional*, ou *cálculo proposicional*, é um formalismo que nos permite determinar o valor lógico de proposições compostas, se soubermos os valores lógicos das proposições simples que a compõem.

A linguagem natural é frequentemente ambígua, e os conectivos lógicos podem ter significados diferentes em sentenças diferentes. Para eliminar essa fonte de confusão, é vantajoso traduzir as proposições para uma notação algébrica, cuja interpretação seja precisamente definida.

Neste livro, representaremos as proposições por letras minúsculas (p, q, r, \dots). Podemos entender estas letras como variáveis que podem ter apenas um de dois valores possíveis, **V** (representando o valor lógico *verdadeiro*) ou **F** (*falso*). Os conectivos lógicos serão representados por sinais algébricos especiais (*operadores*) aplicados a essas variáveis. Os mais importantes são:

- *conjunção*: $p \wedge q$, significando “ p e q ”.
- *disjunção*: $p \vee q$, significando “ p ou q ”.
- *negação*: $\neg p$, significando “não p ”.
- *implicação*: $p \rightarrow q$, significando “se p , então q ”.
- *equivalência*: $p \leftrightarrow q$, significando “ p se, e somente se, q ”.

Nas próximas seções, vamos explicar em detalhes estes operadores lógicos, e definir outros operadores menos usados.

3.1.4 Operador de conjunção

Se p, q são duas proposições, então “ p e q ” também é uma proposição, chamada *conjunção* de p e q . Denotaremos essa proposição por $p \wedge q$. Por definição, o valor lógico de $p \wedge q$ é verdadeiro se p e q são ambos verdadeiros. Se qualquer uma das duas proposições for falsa, ou ambas forem falsas, o valor de $p \wedge q$ é falso. Podemos resumir esta definição por uma tabela, a *tabela-verdade* do operador \wedge :

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Exemplo 3.1: A frase “José compra tijolos e vende casas” é uma conjunção de duas proposições atômicas, “(José compra tijolos) \wedge (José vende casas).”

Note que a palavra “e” em português tem vários sentidos, e nem todos correspondem a conjunção lógica. Por exemplo a frase “Maria gosta de arroz e feijão” não significa “Maria gosta de arroz e Maria gosta de feijão” (uma conjunção de duas proposições), mas sim “Maria gosta de arroz misturado com feijão” (uma proposição atômica).

3.1.5 Operador de disjunção

Se p, q são duas proposições, então “ p ou q ” também é uma proposição, chamada de *disjunção* de p e q . Denotaremos essa proposição por $p \vee q$. Por definição, o valor lógico de $p \vee q$ é verdadeiro se pelo menos uma das duas proposições for verdadeira. Se ambas forem falsas, o valor de $p \vee q$ é falso. A tabela-verdade do operador \vee é

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Exemplo 3.2: A frase “O cliente tem celular ou laptop” é uma disjunção de duas proposições atômicas, “(O cliente tem celular) \vee (O cliente tem laptop)”.

Este conectivo é também chamado de “ou inclusivo”, pois permite que as duas frases sejam verdadeiras. A frase do exemplo acima é verdadeira se o cliente tem apenas celular, apenas laptop, ou celular e laptop.

3.1.6 Operador de negação

A partir de uma proposição p , podemos formar uma nova proposição com o valor lógico oposto ao de p . Essa nova proposição é chamada a *negação* de p e denotada por $\neg p$. A tabela-verdade desse operador é:

p	$\neg p$
V	F
F	V

Em português, a negação pode ser expressa de várias formas, por exemplo acrescentando a palavra “não” antes do verbo ou dizendo que “não é verdade que ...”.

Exemplo 3.3: A frase “A casa é de qualquer cor menos branca.” é uma negação, “ \neg (A casa é branca).”

Exercício 3.1: Uma proposição composta é *viável* ou *possível* se existe uma atribuição de valores verdades para as variáveis da proposição que a torna verdadeira. Verifique quais das proposições abaixo são viáveis.

- $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$.
- $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$.
- $(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (\neg p \vee r \vee s) \wedge (p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee s) \wedge (\neg p \vee \neg r \vee \neg s)$.

3.1.7 Operador de implicação

Sejam p, q duas proposições. A proposição “se p então q ”, que denotaremos por $p \rightarrow q$, é chamada de *implicação* ou *condicional*. O valor lógico de $p \rightarrow q$ é falso apenas se p for verdadeiro e q for falso. Nos demais casos, o valor de $p \rightarrow q$ é verdadeiro. A tabela-verdade desse conectivo é portanto:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Note que em lógica, este conectivo não pressupõe uma relação causal entre p e q . Por exemplo a sentença “se 2 é par então Brasília é a capital do Brasil” é verdadeira apesar de não haver nenhuma relação conhecida entre os dois fatos. Uma outra notação usada para este operador é $p \Rightarrow q$.

Exemplo 3.4: A frase “se José foi para casa, ele perdeu a reunião” contém uma implicação: “(José foi para casa) \rightarrow (José perdeu a reunião).”

A implicação é um dos mais importantes conectivos da lógica e da matemática. Muitos teoremas em matemática estão na forma de implicações: se determinada afirmação p (a *hipótese*, *premissa*, ou *antecedente*) é verdadeira, então outra afirmação q (a *tese*, *conclusão* ou *consequência*) também é verdadeira.

Em português, a implicação pode ser expressa de muitas outras formas:

- se p então q .
- quando p , temos q .

- caso p , vale q .
- q segue de p .
- p implica q .
- q se p .
- q sempre que p .

Em matemática, as seguintes expressões também são muito usadas para indicar a implicação $p \rightarrow q$:

- p é condição suficiente para q .
- p somente se q .
- Uma condição suficiente para q é p .
- p é uma condição mais forte que q .

Dizemos que a implicação $q \rightarrow p$ é a *recíproca* de $p \rightarrow q$. Observe que há casos em que $p \rightarrow q$ é verdadeira, mas sua recíproca $q \rightarrow p$ é falsa; e vice-versa (vide exercício 3.4).

A proposição $(\neg p) \rightarrow (\neg q)$ é chamada de *inversa* de $p \rightarrow q$. Observe que há casos em que $p \rightarrow q$ é verdadeira, mas sua inversa é falsa; e vice-versa (vide exercício 3.5).

Dizemos também que proposição $(\neg q) \rightarrow (\neg p)$ é a *contrapositiva* de $p \rightarrow q$. Pode-se verificar que contrapositiva tem sempre o mesmo valor lógico que a proposição $p \rightarrow q$, quaisquer que sejam os valores lógicos de p e de q (vide exercício 3.6).

Em vista deste resultado, a implicação $p \rightarrow q$ é frequentemente enunciada na forma contrapositiva:

- se não q , então não p .
- se q não vale, então p não vale.
- quando q é falsa, p também é falsa.
- não q implica não p .
- não p se não q .
- p é falsa sempre que q é falsa.
- q é mais fraco que p .
- q é condição necessária para p .
- Uma condição necessária para p é q .

Exercício 3.2: Encontre:

- a) A contrapositiva de $\neg p \rightarrow q$.
- b) A recíproca de $\neg q \rightarrow p$.
- c) A inversa da recíproca de $q \rightarrow \neg p$.
- d) A negação de $p \rightarrow \neg q$.
- e) A recíproca de $\neg p \vee q$.

3.1.8 Operador de equivalência

Se p, q são duas proposições, a proposição “ p se, e somente se, q ” é chamada de *equivalência* ou *bicondicional* de p e q . Denotaremos essa proposição por $p \leftrightarrow q$. O valor lógico de $p \leftrightarrow q$ é verdadeiro quando p e q tem o mesmo valor lógico, e falso caso contrário. A tabela-verdade deste conectivo é

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Exemplo 3.5: A frase “a encomenda será enviada se, e somente se, o cheque tiver fundo” afirma uma equivalência lógica: “[a encomenda será enviada] \leftrightarrow [o cheque tem fundo].”

Outros símbolos usados para este operador são $p \Leftrightarrow q$, $p \equiv q$, e $p = q$.

O conectivo lógico “se e somente se” também é muito usado em matemática, e pode ser expresso de várias outras maneiras; como, por exemplo:

- p é condição necessária e suficiente para q .
- as condições p e q são equivalentes.
- se p então q , e se q então p .
- p implica q , e vice-versa.

Alguns autores usam a abreviação “ p sse q ” (com dois “s”) para significar “ p se e somente se q ”.

3.1.9 Operador de disjunção exclusiva

Se p, q são duas proposições, denotamos por $p \oplus q$ a proposição “ou p ou q , mas não ambos.” Este conectivo é chamado de *disjunção exclusiva* ou p e q . O valor lógico de $p \oplus q$ é verdadeiro se p e q tem valores lógicos opostos, ou seja, exatamente um deles é verdadeiro. A tabela-verdade desse conectivo é

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

É importante observar que, em português, o conectivo “ou” pode significar tanto a disjunção inclusiva (\vee) quanto a disjunção exclusiva (\oplus). Por exemplo, na frase “o original foi enviado pelo correio, ou [o original foi enviado] pelo malote,” entende-se que o “ou” é exclusivo, pois o original não pode ter sido enviado pelos dois meios. Por outro lado, na frase “a bateria está descarregada ou o tanque está vazio” o “ou” deve ser entendido como inclusivo, pois nada impede que as duas condições sejam verdadeiras. A interpretação correta geralmente depende do contexto, e em alguns casos pode ser impossível determinar qual dos dois sentidos é o que o autor da frase pretendia.

3.1.10 Precedência dos operadores lógicos

Em uma proposição que usa dois ou mais operadores lógicos, como $p \vee q \wedge r$, a ordem em que eles devem ser aplicados é muito importante. Podemos sempre usar parênteses para indicar a ordem correta, por exemplo $(p \vee q) \wedge r$ ou $p \vee (q \wedge r)$. Observe que estas duas proposições podem ter valores lógicos diferentes, para certas proposições p , q , e r .

Assim como na álgebra, é útil estabelecer *regras de precedência* entre operadores, que determinam uma ordem convencional de aplicação mesmo na ausência de parênteses, como na proposição $p \vee q \wedge r$.

A tabela a seguir estabelece as precedências tradicionais dos operadores lógicos.

Operador	Precedência
\neg	1
\wedge	2
\vee, \oplus	3
$\rightarrow, \leftrightarrow$	4

Assim, por exemplo, a proposição $\neg p \wedge q \rightarrow r \oplus s \wedge u$ deve ser entendida como $((\neg p) \wedge q) \rightarrow (r \oplus (s \wedge u))$.

Para memorizar as prioridades relativas de \wedge e \vee , basta lembrar que \wedge (“e”), na álgebra de Boole, era representado por multiplicação; enquanto que \vee (“ou”) era representado por uma soma modificada. Assim, a proposição $p \vee q \wedge r$, por analogia com $x + y \times z$, deve ser entendida como $p \vee (q \wedge r)$ e não como $(p \vee q) \wedge r$.

Em matemática, diz-se que uma operação \star é *associativa* se $(x \star y) \star z$ é igual a $x \star (y \star z)$, quaisquer que sejam x , y , e z . Nesse caso, podemos omitir os parênteses dessas duas fórmulas, e escrever simplesmente $x \star y \star z$. A soma e a multiplicação de números reais, por exemplo, são operações associativas; enquanto que a subtração não é.

Dentre os conectivos lógicos que vimos até agora, \vee , \wedge e \oplus são associativos. Portanto, podemos escrever $p \vee q \vee r$, $p \wedge q \wedge r$ ou $p \oplus q \oplus r$, sem risco de ambiguidade. Por outro lado, a fórmula $p \rightarrow q \rightarrow r$ é ambígua, pois $(p \rightarrow q) \rightarrow r$ não é equivalente a $p \rightarrow (q \rightarrow r)$. (Isto pode ser verificado construindo as tabelas-verdade.)

É tradicional considerar \oplus como tendo menos prioridade que \wedge . (Em parte, isso se deve ao uso de “+” para denotar \oplus em certas áreas da matemática.) Por outro lado, não há uma tradição forte para interpretar combinações de \oplus com \vee , como $p \oplus q \vee r$.

Alguns autores usam a convenção de que fórmulas com dois ou mais operadores não associativos de mesma prioridade, como $p \rightarrow q \rightarrow r$, devem ser avaliadas da esquerda para a direita; ou seja $(p \rightarrow q) \rightarrow r$. Note que esta convenção também é usada em álgebra: a fórmula $x - y - z$ deve ser entendida como $(x - y) - z$, e não como $x - (y - z)$. A mesma regra poderia ser usada para interpretar $p \oplus q \vee r$. Mas, por via das dúvidas, é aconselhável usar parênteses nesses casos. O mesmo vale para \rightarrow em relação a \leftrightarrow , como $p \rightarrow q \leftrightarrow r$. Para evitar equívocos, é aconselhável sempre usar parênteses.

O conectivo \leftrightarrow também é associativo portanto as fórmulas $(p \leftrightarrow q) \leftrightarrow r$ e $p \leftrightarrow (q \leftrightarrow r)$ são equivalentes, e portanto $p \leftrightarrow q \leftrightarrow r$ não é ambígua. Porém muitos autores tem o hábito de usar a notação $p \leftrightarrow q \leftrightarrow r$ para significar $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$, ou seja, que as três proposições p , q , e r tem o mesmo valor lógico. Entretanto, esta afirmação não equivale nem a $(p \leftrightarrow q) \leftrightarrow r$, nem a $p \leftrightarrow (q \leftrightarrow r)$. O leitor precisa tomar cuidado para não se confundir com esse abuso de notação.

3.2 Afirmações auto-referentes

Já mencionamos que a afirmações que referem a si mesmas, como “esta sentença é falsa”, não são proposições lógicas. Tais afirmações, relacionadas com o Paradoxo do Barbeiro, sempre foram um problema para a lógica matemática, que não tem maneira satisfatórias de lidar com elas.

Este problema surge mesmo quando há várias afirmações que se referenciam entre si. Por exemplo, na frase “a sentença seguinte é falsa, e a sentença anterior é verdadeira”, embora possa ser analisada como uma conjunção $p \wedge q$, não é uma afirmação lógica porque p é uma afirmação sobre q e vice-versa. Um exemplo mais elaborado é o seguinte

Exemplo 3.6: Considere uma lista de 100 proposições, p_0, p_1, \dots, p_{99} , onde cada proposição p_n diz “exatamente n das proposições desta lista são falsas.”

Exercício 3.3:

Sejam p e q as proposições “a eleição foi decidida” e “os votos foram contados”, respectivamente. Expresse cada uma das proposições compostas a seguir como uma sentença em português.

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

Exercício 3.4: Mostre, pelas tabelas-verdade, que há casos em que $p \rightarrow q$ é verdadeira, mas sua recíproca $q \rightarrow p$ é falsa; e vice-versa.

Exercício 3.5: Mostre, pelas tabelas-verdade, que há casos em que $p \rightarrow q$ é verdadeira, mas sua inversa $(\neg p) \rightarrow (\neg q)$

Exercício 3.6: Mostre, pelas tabelas-verdade, que a proposição $p \rightarrow q$ e sua contrapositiva $(\neg q) \rightarrow (\neg p)$ tem sempre o mesmo valor lógico, quaisquer que sejam os valores lógicos de p e de q .

Exercício 3.7: Mostre que a inversa de uma implicação $p \rightarrow q$ é a contrapositiva da recíproca.

Exercício 3.8: Mostre que a inversa de uma implicação $p \rightarrow q$ é a recíproca da sua contrapositiva.

Exercício 3.9: Considere que p , $\neg q$ e r são proposições verdadeiras. Verifique quais das afirmações são verdadeiras.

- a) $p \rightarrow q$.
- b) $q \rightarrow p$.
- c) $p \rightarrow (q \vee r)$.
- d) $p \leftrightarrow q$.
- e) $p \leftrightarrow r$.
- f) $(p \vee q) \rightarrow p$.
- g) $(p \wedge q) \rightarrow q$.

Exercício 3.10: Um conectivo muito importante para projeto de circuitos lógicos é o operador *não-e* ou (*nand*), que denotaremos por $\bar{\wedge}$, definido por $p \bar{\wedge} q = \neg(p \wedge q)$. De maneira análoga temos o operador *não-ou* ou (*nor*), denotado por $\bar{\vee}$, e definido por $p \bar{\vee} q = \neg(p \vee q)$. Construa as tabelas-verdade dos operadores $\bar{\wedge}$ e $\bar{\vee}$.

Exercício 3.11: Encontre fórmulas envolvendo os conectivos \wedge , \vee e \neg para as variáveis x e y da tabela-verdade abaixo:

p	q	x	y
V	V	V	F
V	F	V	V
F	V	F	V
F	F	V	F

Exercício 3.12: Construa a tabela-verdade de cada uma das proposições:

- a) $(p \wedge q) \rightarrow (p \vee q)$.
- b) $(p \rightarrow q) \rightarrow (q \rightarrow p)$.
- c) $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$.
- d) $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$.
- e) $(p \oplus q) \rightarrow (p \oplus \neg q)$.

3.3 Manipulação lógica de proposições

O objetivo da lógica proposicional é identificar as deduções e transformações de proposições compostas cuja validade independe da natureza das suas proposições atômicas, e dos valores lógicos destas.

Por exemplo, veremos mais adiante que qualquer proposição composta da forma $p \wedge (p \wedge q)$ pode ser substituída por $p \wedge q$; pois, qualquer que sejam as proposições p e q , os valores lógicos de $p \wedge (p \wedge q)$ e $p \wedge q$ são sempre iguais. Nesta seção, veremos as principais regras deste tipo.

3.3.1 Tautologias e contradições

Uma *tautologia* é uma proposição composta que é sempre verdadeira, quaisquer que sejam os valores lógicos das proposições simples que a compõem. Ou seja, uma proposição composta é uma tautologia se e somente se a coluna de resultado de sua tabela-verdade contém somente valores lógicos verdadeiros (**V**).

Por exemplo, a proposição $p \vee (\neg p)$ tem a seguinte tabela-verdade:

p	$\neg p$	$p \vee (\neg p)$
V	F	V
V	F	V
F	V	V
F	V	V

Podemos concluir então que a proposição $p \vee (\neg p)$ é uma tautologia. Observe que a veracidade de uma tautologia é uma propriedade de sua forma, e é independente dos significados de suas proposições simples. A tautologia mais simples é **V**.

Uma *contradição* é uma proposição composta que é sempre falsa, quaisquer que sejam os valores lógicos das suas proposições atômicas. Portanto, uma proposição composta é uma contradição se, e somente se, sua tabela-verdade contém somente **F** na sua coluna final. É fácil ver que a proposição $p \wedge (\neg p)$ é uma contradição.

Em particular, a negação de uma tautologia é sempre uma contradição, e a negação de uma contradição é uma tautologia. A contradição mais simples é **F**.

Exercício 3.13: Construa as tabelas-verdade das proposições abaixo, e determine se elas são tautologias, contradições, ou nem uma nem outra.

- $(p \wedge \neg q) \rightarrow (q \vee \neg p)$.
- $\neg p \rightarrow p$.
- $\neg p \leftrightarrow p$.
- $(p \wedge \neg p) \rightarrow p$.
- $(p \wedge \neg p) \rightarrow q$.
- $(p \wedge \neg q) \leftrightarrow (p \rightarrow q)$.
- $((p \oplus q) \oplus (q \oplus p))$.

Exercício 3.14: Construa as tabelas-verdade das proposições abaixo, e determine se elas são tautologias, contradições, ou nem uma nem outra. Note que as fórmulas dependem de 3 variáveis, portanto a tabela verdade tem $2^3 = 8$ linhas.

- g) $((p \rightarrow q) \leftrightarrow r) \leftrightarrow (p \rightarrow (q \leftrightarrow r))$.
 i) $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

3.3.2 Equivalência lógica

Duas proposições compostas p e q são ditas *logicamente equivalentes* se elas tem valores lógicos iguais, para qualquer combinação de valores lógicos que sejam atribuídos às suas proposições atômicas. Em outras palavras, p e q são logicamente equivalentes se e somente se $p \leftrightarrow q$ é uma tautologia.

Por exemplo, podemos verificar, pela tabela-verdade, que as proposições compostas p e $\neg(\neg p)$ são equivalentes, ou seja, que $p \leftrightarrow (\neg(\neg p))$ é uma tautologia:

p	$\neg p$	$\neg(\neg p)$	$p \leftrightarrow (\neg(\neg p))$
V	F	V	V
F	V	F	V

Este resultado é conhecido como *lei da negação dupla*.

Como outro exemplo, podemos verificar que a proposição $p \leftrightarrow q$ é equivalente a $(p \rightarrow q) \wedge (q \rightarrow p)$; ou seja, que $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$ é uma tautologia:

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$
V	V	V	V	V	V	V
V	F	F	F	V	F	V
F	V	F	V	F	F	V
F	F	V	V	V	V	V

Assim como a propriedade de ser tautologia ou de ser contradição, a equivalência lógica de duas proposições depende apenas da sua forma, e não depende do significado das proposições atômicas que ocorrem nela. Assim, por exemplo, a proposição $p \leftrightarrow q$ pode ser verdadeira, dependendo das proposições p e q ; mas nem por isso p é logicamente equivalente a q .

Podemos dizer, portanto, que uma tautologia é uma proposição logicamente equivalente a **V**; e uma contradição é uma proposição logicamente equivalente a **F**.

3.3.3 Equivalências lógicas importantes

A seguir listaremos algumas equivalências lógicas importantes. O leitor pode se convencer da veracidade delas construindo as respectivas tabelas-verdade.

- *Leis de elemento identidade:*

- $p \wedge \mathbf{V}$ equivale a p
- $p \vee \mathbf{F}$ equivale a p

- $p \leftrightarrow \mathbf{V}$ equivale a p
- $p \oplus \mathbf{F}$ equivale a p
- *Leis da idempotência:*
 - $p \wedge p$ equivale a p
 - $p \vee p$ equivale a p
- *Leis de dominação:*
 - $p \vee \mathbf{V}$ equivale a \mathbf{V}
 - $p \wedge \mathbf{F}$ equivale a \mathbf{F}
- *Leis da comutatividade:*
 - $p \vee q$ equivale a $q \vee p$
 - $p \wedge q$ equivale a $q \wedge p$
 - $p \leftrightarrow q$ equivale a $q \leftrightarrow p$
 - $p \oplus q$ equivale a $q \oplus p$
- *Leis da associatividade:*
 - $(p \vee q) \vee r$ equivale a $p \vee (q \vee r)$
 - $(p \wedge q) \wedge r$ equivale a $p \wedge (q \wedge r)$
 - $(p \leftrightarrow q) \leftrightarrow r$ equivale a $p \leftrightarrow (q \leftrightarrow r)$
 - $(p \oplus q) \oplus r$ equivale a $p \oplus (q \oplus r)$
- *Leis da distributividade:*
 - $p \vee (q \wedge r)$ equivale a $(p \vee q) \wedge (p \vee r)$
 - $p \wedge (q \vee r)$ equivale a $(p \wedge q) \vee (p \wedge r)$
 - $p \wedge (q \oplus r)$ equivale a $(p \wedge q) \oplus (p \wedge r)$
- *Leis de De Morgan:*
 - $\neg(p \wedge q)$ equivale a $\neg p \vee \neg q$
 - $\neg(p \vee q)$ equivale a $\neg p \wedge \neg q$
- *Leis da implicação*
 - $(p \rightarrow q)$ equivale a $(\neg p \vee q)$
 - $\neg(p \rightarrow q)$ equivale a $(p \wedge \neg q)$
- *Lei da contrapositiva:*
 - $(p \rightarrow q)$ equivale a $(\neg q) \rightarrow (\neg p)$

- *Lei da redução ao absurdo:*

$$- p \rightarrow q \text{ equivale a } (p \wedge \neg q) \rightarrow \mathbf{F}$$

Exercício 3.15: Verifique cada uma das equivalências acima, construindo a tabela-verdade para as duas proposições.

Exercício 3.16: Verifique quais das seguintes afirmações são corretas:

- $(\neg p \wedge (p \vee q))$ é logicamente equivalente a q .
- $((p \rightarrow q) \rightarrow r)$ é logicamente equivalente a $(p \rightarrow (q \rightarrow r))$.
- $((p \leftrightarrow q) \leftrightarrow r)$ é logicamente equivalente a $(p \leftrightarrow (q \leftrightarrow r))$.
- $p \rightarrow (q \wedge r)$ é logicamente equivalente a $(p \rightarrow q) \wedge (p \rightarrow r)$.
- $(p \vee q) \rightarrow r$ é logicamente equivalente a $(p \rightarrow r) \wedge (q \rightarrow r)$.

Exercício 3.17: Use a tabela-verdade para provar as *leis de absorção*:

- $(p \vee (p \wedge q))$ é logicamente equivalente a p .
- $(p \wedge (p \vee q))$ é logicamente equivalente a p .

Exercício 3.18: Quais proposições são logicamente equivalentes?

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

Exercício 3.19: Encontre uma fórmula usando apenas os conectivos \wedge e \neg que seja logicamente equivalente a $(r \wedge \neg p) \vee (q \wedge \neg r)$. Justifique sua resposta com a tabela-verdade.

Exercício 3.20: Encontre uma fórmula usando apenas os conectivos \rightarrow e \neg que seja logicamente equivalente a $p \wedge q$. Justifique sua resposta com a tabela-verdade.

Exercício 3.21: Encontre uma proposição usando os conectivos \rightarrow e \oplus que seja logicamente equivalente a $p \vee q$. Justifique sua resposta com a tabela-verdade.

Exercício 3.22: Use as leis de equivalência lógica vistas acima para encontrar fórmulas mais simples que sejam logicamente equivalentes às seguintes proposições:

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

3.3.4 Implicação lógica

Sejam p e q duas proposições. Dizemos que p *implica logicamente* q se $p \rightarrow q$ é uma tautologia. Nesse caso, dizemos também que $p \rightarrow q$ é uma *implicação lógica* ou q é uma *consequência lógica de* p . Mais geralmente, sejam p_1, p_2, \dots, p_n uma coleção de proposições. Dizemos que essas proposições *implicam logicamente* q se $(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$ é uma tautologia.

Observe que se uma implicação $p \rightarrow q$ é verdadeira, sua conclusão q pode ser verdadeira ou falsa; mas se tanto a implicação quanto a hipótese p são verdadeiras, então a conclusão q deve ser verdadeira. Isto é, as proposições p e $p \rightarrow q$ implicam logicamente q . Isso significa que, se estabelecemos de alguma forma que p é verdadeira, e que $p \rightarrow q$ é verdadeira, podemos concluir que q é verdadeira. Esta implicação lógica é chamada *lei do modus ponens* e é frequentemente usada nas demonstrações de teoremas em matemática. Listaremos algumas implicações lógicas mais conhecidas. As letras p, q, r representam proposições arbitrárias.

- *Lei da adição:*
 - p implica logicamente $p \vee q$
- *Lei da simplificação:*
 - $p \wedge q$ implica logicamente p
- *Lei do modus ponens:*
 - p e $p \rightarrow q$ implicam logicamente q
- *Lei do modus tollens:*
 - $p \rightarrow q$ e $\neg q$ implicam logicamente $\neg p$
- *Silogismo hipotético:*
 - $p \rightarrow q$ e $q \rightarrow r$ implicam logicamente $p \rightarrow r$
- *Silogismo disjuntivo:*
 - $p \vee q$ e $\neg p$ implicam logicamente q
- *Demonstração por absurdo:*
 - $p \rightarrow \mathbf{F}$ implica logicamente $\neg p$

Exercício 3.23: Verifique cada uma das implicações acima, construindo a tabela-verdade para as duas proposições.

Exercício 3.24: Verifique quais das seguintes afirmações são corretas:

- a) $(p \rightarrow (q \vee r))$ implica logicamente em $(p \rightarrow q)$.
- b) $(p \rightarrow q)$ implica logicamente em $(r \wedge p \rightarrow q)$.

- c) $((p \vee q) \rightarrow r)$ implica logicamente em $(p \rightarrow r)$.
- d) $((p \rightarrow q) \wedge \neg p)$ implica logicamente em $\neg q$.
- e) $(p \leftrightarrow q)$ implica logicamente em $(p \rightarrow q)$.
- f) $(p \rightarrow q)$ implica logicamente em $(p \leftrightarrow q)$.
- g) $(p \rightarrow q)$ implica logicamente em q .
- h) $(p \vee q) \wedge (\neg p \vee r)$ implica logicamente em $(q \vee r)$.
- i) $(p \rightarrow q) \wedge (q \rightarrow r)$ implica logicamente em $(p \rightarrow r)$.

3.3.5 Equivalência em contexto específico

As equivalências e implicações lógicas acima são absolutas, isto é, podem ser usadas quaisquer que sejam as proposições simples representadas pelas variáveis.

Neste sentido, por exemplo as fórmulas $p \leftrightarrow q$ e $p \wedge q$ não são equivalentes; pois, quando substituimos $p = \mathbf{F}$ e $q = \mathbf{F}$, a primeira é verdadeira e a segunda é falsa. Porém, se soubermos de alguma maneira, que a afirmação $p \vee q$ é verdadeira, então a combinação $p = \mathbf{F}$ e $q = \mathbf{F}$ não pode ocorrer. As tabelas-verdade dessas fórmulas são:

p	q	$p \leftrightarrow q$	$p \wedge q$	$p \vee q$
F	F	V	F	F
F	V	F	F	V
V	F	F	F	V
V	V	V	V	V

Observe que, em todos os casos onde a fórmula $p \vee q$ é verdadeira, a afirmação $p \leftrightarrow q$ tem o mesmo valor lógico de que $p \wedge q$. Portanto, *supondo que $p \vee q$ é verdade*, podemos dizer que as duas outras proposições são logicamente equivalentes.

Em geral, podemos dizer que duas proposições compostas são equivalentes se tiverem o mesmo valor lógico para todas as combinações de valores de suas proposições simples *que forem permitidas pelos fatos conhecidos sobre as mesmas*.

3.4 Síntese de proposições

3.4.1 Formas normais disjuntivas e conjuntivas

Dada uma tabela-verdade com determinadas variáveis lógicas, é sempre possível construir uma proposição composta com essas mesmas variáveis que tem essa tabela-verdade. Podemos construir essa proposição tomando todas as linhas da tabela em que o resultado desejado é verdadeiro, e escrevendo para cada linha uma fórmula lógica que é verdadeira para essa combinação de valores das variáveis, e falsa para todas as outras combinações. Para isto, podemos usar uma conjunção de variáveis ou suas negações. A disjunção de todas essas fórmulas é a proposição desejada.

Por exemplo, suponha que queremos construir uma proposição r que tem esta tabela-verdade:

p	q	r
F	F	F
F	V	V
V	F	V
V	V	F

Para a segunda linha, precisamos de uma fórmula que seja **V** apenas quando $p = \mathbf{F}$ e $q = \mathbf{V}$. Para isso podemos usar a fórmula $(\neg p) \wedge q$. Para a terceira linha, a fórmula é $p \wedge (\neg q)$. A proposição desejada é então

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

A fórmula obtida desta maneira — uma disjunção de conjunções, cujos termos são variáveis ou suas negações — é chamada de *forma normal disjuntiva*. A construção acima nos permite concluir que toda proposição composta tem uma forma normal disjuntiva que lhe é logicamente equivalente.

Outra maneira de construir uma proposição a partir de sua tabela-verdade é considerar cada linha em que o resultado desejado é **F**, e escrever uma fórmula que é falsa apenas para essa combinação de variáveis. Esta fórmula pode ser uma disjunção das variáveis e suas negações. A conjunção dessas fórmulas é a proposição desejada. A partir da tabela acima, por exemplo, obteríamos

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

A fórmula assim obtida é chamada de *forma normal conjuntiva*.

Exercício 3.25: Considere a tabela-verdade abaixo:

p	q	r	s
F	F	F	F
F	F	V	V
F	V	F	V
F	V	V	F
V	F	F	V
V	F	V	F
V	V	F	F
V	V	V	F

1. Construa uma proposição composta na forma normal disjuntiva com essa tabela-verdade.
2. Idem, na forma normal conjuntiva.

3.4.2 Sistemas completos de operadores

A construção da forma normal disjuntiva (ou conjuntiva) permite concluir que toda proposição composta, usando quaisquer conectivos, é logicamente equivalente a outra proposição que usa apenas os conectivos \vee , \wedge e \neg . Dizemos então que estes três conectivos formam um *sistema completo* de operadores lógicos.

Exercício 3.26: Prove que os conectivos \wedge e \neg , sozinhos, constituem um sistema completo de operadores lógicos. Idem para \vee e \neg .

Exercício 3.27: Prove que os conectivos \oplus e \wedge , sozinhos, constituem um sistema completo de operadores lógicos. (Dica: prove que é possível obter o operador \neg combinando esses dois operadores.)

Exercício 3.28: Prove que o conectivo $\bar{\wedge}$ (não-e), sozinho, constitui um sistema completo de operadores lógicos. Idem para $\bar{\vee}$ (não-ou).

3.5 Dualidade lógica

Seja p uma proposição que usa apenas os conectivos \vee , \wedge , e \neg . A *proposição dual* é obtida a partir de p trocando-se toda ocorrência de \vee por \wedge , e vice-versa; bem como toda ocorrência de **T** por **F**, e vice-versa. Por exemplo, a dual da proposição $(p \wedge \neg q) \vee r$ é $(p \vee \neg q) \wedge r$. A dual de uma proposição p é geralmente denotada por p^* . Note que $(p^*)^*$, a dual da dual, é a proposição original p .

Em geral, p e p^* não são logicamente equivalentes. Entretanto, se p é uma tautologia, p^* é uma contradição, e vice-versa. Além disso, prova-se que se duas proposições p e q são equivalentes, então p^* e q^* são equivalentes, e vice-versa. Esta propriedade nos permite obter equivalências lógicas a partir de equivalências já demonstradas.

Por exemplo, considere as duas leis de distributividade, de \wedge sobre \vee e \vee sobre \wedge :

$$p \wedge (q \vee r) \text{ é equivalente a } (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \text{ é equivalente a } (p \vee q) \wedge (p \vee r)$$

Uma vez provada a primeira equivalência, não precisamos provar a segunda: basta observar que $p \vee (q \wedge r)$ é a proposição dual de $p \wedge (q \vee r)$, e $(p \vee q) \wedge (p \vee r)$ é a dual de $(p \wedge q) \vee (p \wedge r)$.

Exercício 3.29: Escreva a proposição dual de $(p \wedge q) \vee \neg(p \vee r)$.

Exercício 3.30: Qual é a relação entre as tabelas-verdade de uma proposição p e de sua proposição dual p^* ?

Exercício 3.31: Encontre uma proposição composta com duas variáveis lógicas, que seja logicamente equivalente a sua proposição dual usando apenas os operadores \vee , \wedge e \neg .

Exercício 3.32: Para definir o dual de um operador lógico binário qualquer \odot , basta encontrar uma fórmula equivalente a $p \odot q$ que use apenas os operadores \wedge , \vee , e \neg , e definir um operador \otimes tal que $p \otimes q$ seja equivalente à proposição dual dessa fórmula. Use este processo para definir os operadores duais de \leftrightarrow , \oplus , \rightarrow , $\bar{\vee}$ e $\bar{\wedge}$. Em cada caso, determine se o dual é um operador conhecido.

3.6 Lógica de Predicados

Uma *proposição aberta* é uma proposição que depende de uma ou mais variáveis, por exemplo

- “ $x + 1$ é maior que x ”.

- “o quadrado de x é 16”.
- “ x é um número primo”.
- “ x é maior que y ”.
- “ $x + y = 2x + z$ ”

Em geral, o valor lógico de uma proposição aberta depende dos valores das variáveis que nela ocorrem. Por exemplo, a frase “ x é maior que y ” é verdadeira se os valores de x e y forem 7 e 4, mas é falsa se os valores forem 10 e 21.

Para certos valores, a frase pode até mesmo não fazer sentido: por exemplo, “ x é maior que y ” não faz sentido se x e y forem números complexos, ou se x for uma matriz e y for um número real. Com esta ressalva, sempre que substituimos as variáveis de uma proposição aberta por valores aceitáveis, obtemos uma *proposição fechada*, que não depende de nenhuma variável — e que portanto pode ser tratada como uma proposição atômica do cálculo proposicional.

No restante deste capítulo, usaremos letras minúsculas x, y, z para denotar variáveis. Usaremos também letras maiúsculas P, Q, R, \dots , seguidas por uma lista de variáveis distintas entre parênteses, para denotar proposições abertas que dependem dessas variáveis. Por exemplo, a notação $P(x)$ pode representar a frase “ x é um número primo”, e $Q(x, y)$ pode representar “ y é maior que x ”.

Os símbolos P, Q, R, \dots são chamados de *predicados*, e podem ser entendidos como funções que, dados valores das variáveis, assumem um valor lógico (**F** ou **V**). Como na álgebra, depois de definido um predicado $P(x_1, x_2, \dots, x_n)$, usaremos a notação $P(v_1, v_2, \dots, v_n)$ para indicar a substituição da variável x_1 pelo valor v_1 , x_2 pelo valor v_2 , etc.. Por exemplo, se $Q(x, y)$ foi definido como a proposição aberta “ y é maior que x ”, então $Q(3, z + 1)$ representa a afirmação “ $z + 1$ é maior que 3”. Assim como na álgebra, supõe-se que todas as ocorrências da mesma variável na proposição são substituídas pelo mesmo valor.

3.6.1 Quantificação universal

A substituição de variáveis por valores explícitos não é a única maneira de transformar uma proposição aberta em uma proposição atômica. Outra maneira é a chamada *quantificação universal*, que é uma afirmação do tipo “para todo x no conjunto D , $P(x)$ ”.

Denotaremos esta frase por $(\forall x \in D)P(x)$. Nesta frase, D (o *domínio* da quantificação) pode ser qualquer conjunto previamente definido, x pode ser qualquer variável, e $P(x)$ qualquer proposição que depende dessa variável, que tenha valor lógico bem definido sempre que x for substituído por um elemento de D .

Por definição, a frase $(\forall x \in D)P(x)$ é verdadeira se, e somente se, a proposição $P(x)$ for sempre verdadeira quando substituirmos variável x por qualquer elemento do conjunto D . Se houver um (ou mais de um) elemento de D que torna $P(x)$ falsa quando atribuído à variável x , então a frase $(\forall x \in D)P(x)$ é falsa.

Por exemplo, se $P(x)$ representa a frase “ $x + 1$ é maior que x ”, então a frase “ $(\forall x \in \mathbb{Z})P(x)$ ” é verdadeira, pois, se substituirmos x por qualquer número inteiro, a afirmação $P(x)$ será sempre verdadeira.

Por outro lado, se $P(x)$ representa a frase “ x é um número primo”, então a frase “ $(\forall x \in \mathbb{N}) P(x)$ ” é falsa; pois, embora as afirmações $P(3)$ e $P(17)$ sejam verdadeiras, a afirmação $P(6)$ (por exemplo) é falsa.

Em geral, se o domínio D é um conjunto finito, com elementos v_1, v_2, \dots, v_n , então a frase $(\forall x \in D) P(x)$ é equivalente a $P(v_1) \wedge P(v_2) \wedge \dots \wedge P(v_n)$.

Exercício 3.33: Sejam \mathbb{N} o conjunto dos números naturais, e suponha que $P(x)$ significa “ x é par”, $Q(x)$ significa “ x é divisível por 3” e $R(x)$ significa “ x é divisível por 4”. Escreva em linguagem natural (português) cada uma das proposições a seguir, e determine seu valor-verdade:

- a) $(\forall x \in \mathbb{N}) P(x)$.
- b) $(\forall x \in \mathbb{N}) P(x) \vee Q(x)$.
- c) $(\forall x \in \mathbb{N}) P(x) \rightarrow Q(x)$.
- d) $(\forall x \in \mathbb{N}) P(x) \vee R(x)$.
- e) $(\forall x \in \mathbb{N}) P(x) \wedge R(x)$.
- f) $(\forall x \in \mathbb{N}) R(x) \rightarrow P(x)$.
- g) $(\forall x \in \mathbb{N}) P(x) \rightarrow \neg Q(x)$.
- h) $(\forall x \in \mathbb{N}) P(x) \rightarrow P(x + 2)$.
- i) $(\forall x \in \mathbb{N}) R(x) \rightarrow R(x + 4)$.
- j) $(\forall x \in \mathbb{N}) Q(x) \rightarrow Q(x + 1)$.

3.6.2 Quantificação existencial

Outra maneira de transformar uma proposição aberta em fechada é através da *quantificação existencial*, que tem a forma “existe um x no conjunto D tal que $P(x)$ ”.

Denotaremos esta frase por $(\exists x \in D) P(x)$. Aqui também, o domínio D da quantificação pode ser qualquer conjunto já definido; x pode ser qualquer variável; e $P(x)$ qualquer proposição que depende dessa variável.

Por definição, a frase “ $(\exists x \in D) P(x)$ ” é verdadeira se, e somente se, existir pelo menos um elemento de D que, atribuído à variável x , torna a afirmação $P(x)$ verdadeira. A frase “ $(\exists x \in D) P(x)$ ” é falsa se, e somente se, não existe nenhum elemento de D com essa propriedade.

Se D é um conjunto finito com elementos v_1, v_2, \dots, v_n , então a frase $(\exists x \in D) P(x)$ é equivalente a $P(v_1) \vee P(v_2) \vee \dots \vee P(v_n)$.

Como exemplo, denotemos por $P(x)$ o predicado “ x é um número primo”. A proposição $(\exists x \in \mathbb{N}) P(x)$ é verdadeira, pois, por exemplo, a afirmação $P(7)$ (“7 é um número primo”) é verdadeira, e 7 é um elemento de \mathbb{N} . Por outro lado, se $Q(y)$ é a proposição aberta “ y é igual a $y + 1$ ”, então a frase “ $(\exists y \in \mathbb{R}) Q(y)$ ” é falsa; pois, qualquer número real que for atribuído a y , a afirmação $Q(y)$ (“ y é igual a $y + 1$ ”) é falsa.

Exercício 3.34: Sejam \mathbb{N} o conjunto dos números naturais, e suponha que $P(x)$ significa “ x é par”, $Q(x)$ significa “ x é divisível por 3” e $R(x)$ significa “ x é divisível por 4”. Escreva em linguagem natural (português) cada uma das proposições a seguir, e determine seu valor-verdade:

- a) $(\exists x \in \mathbb{N}) R(x)$

- b) $(\exists x \in \mathbb{N}) P(x) \vee Q(x)$.
- c) $(\exists x \in \mathbb{N}) P(x) \rightarrow Q(x)$.
- d) $(\exists x \in \mathbb{N}) Q(x) \rightarrow Q(x + 1)$.
- e) $(\exists x \in \mathbb{N}) P(x) \rightarrow Q(x + 1)$.

Exercício 3.35: Sejam \mathbb{N} o conjunto dos números naturais, $P(x, y)$ é “ $x + 2 > y$ ”. Escreva as proposições listadas abaixo em linguagem natural (português) e atribua o valor-verdade correspondente a cada uma delas:

- a) $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N}) P(x, y)$.
- b) $(\exists x \in \mathbb{N})(\exists y \in \mathbb{N}) P(x, y)$.
- c) $(\exists y \in \mathbb{N})(\forall x \in \mathbb{N}) P(x, y)$.

3.6.3 Quantificador de existência e unicidade

Na matemática são comuns afirmações do tipo “existe um *único* x no conjunto D tal que $P(x)$.” Esta afirmação é frequentemente denotada por $(\exists! x \in D) P(x)$.

Observe que, assim como \exists pode ser visto como uma disjunção inclusiva \vee , o quantificador $\exists!$ pode ser visto como uma disjunção exclusiva \oplus . Ou seja, se $D = \{x_1, x_2, \dots, x_n\}$, a proposição $(\exists! x \in D) P(x)$ significa que uma, e apenas uma, das afirmações $P(x_1), P(x_2), \dots, P(x_n)$ é verdadeira.

Porém, note que esta afirmação *não* é equivalente a $P(x_1) \oplus P(x_2) \oplus \dots \oplus P(x_n)$. Pode-se verificar que esta afirmação significa que um número ímpar desses termos são verdadeiros.

Toda fórmula $(\exists! x \in D) P(x)$ pode ser escrita em termos dos quantificadores já definidos:

$$((\exists x \in D) P(x)) \wedge ((\forall x \in D)(\forall y \in D) ((P(x) \wedge P(y)) \rightarrow x = y))$$

3.6.4 Quantificação sobre o conjunto vazio

A afirmação “existe um estudante com mais de duzentos anos que gosta de física” é obviamente falsa; pois nem sequer existem estudantes com essa idade, muito menos que gostem de física. Esta afirmação pode ser escrita $(\exists x \in D) P(x)$, onde D é o conjunto dos estudantes com mais de duzentos anos de idade, e $P(x)$ denota a afirmação “ x gosta de física”. De modo geral, se o domínio D é vazio, a afirmação “ $(\exists x \in D) P(x)$ ” é falsa, qualquer que seja o predicado P .

Considere agora a afirmação: “todos os estudantes com mais de duzentos anos de idade gostam de física.” Qual o valor lógico desta frase?

Na notação acima, esta afirmação pode ser escrita $(\forall x \in D) P(x)$. A questão é: qual o valor lógico da afirmação “ $P(x)$ é verdadeira, para qualquer elemento x de D ”, se D não tem nenhum elemento?

Verifica-se que, quando o domínio D é vazio, a interpretação mais consistente é considerar a frase $(\forall x \in D) P(x)$ verdadeira, qualquer que seja o predicado P . Dizemos que tais afirmações são verdadeiras por vacuidade. Em particular, a frase “todos os estudantes com mais de duzentos anos de idade gostam de física” deve ser considerada verdadeira.

Por outro lado,

3.6.5 Cálculo de predicados

A área da lógica que trata de predicados e quantificadores é chamada *cálculo de predicados*. Assim como no cálculo proposicional, no cálculo de predicados estudam-se as regras de raciocínio que valem para *quaisquer* predicados. Em particular, estamos interessados em *equivalências lógicas* e *implicações lógicas* entre proposições com quantificadores.

Assim como no cálculo proposicional, definimos uma *tautologia* do cálculo de predicados como sendo uma proposição com domínios e predicados simbólicos que é verdadeira quaisquer que sejam as definições que adotemos para os mesmos. Um exemplo trivial é a proposição “ $(\forall x \in D) P(x) \vee \neg P(x)$ ”. Dizemos também que duas proposições quantificadas p e q são *logicamente equivalentes* se $p \leftrightarrow q$ é uma tautologia, e que p *implica logicamente* q se $p \rightarrow q$ é uma tautologia. Por outro lado, uma *contradição* é uma proposição que é falsa quaisquer que sejam as definições adotadas para seus predicados; como, por exemplo, “ $(\exists x \in D) P(x) \wedge \neg P(x)$ ”.

3.6.6 Negação de quantificadores

Um exemplo importante de equivalência lógica no cálculo de predicados são as regras para *negação de quantificadores*:

- $\neg[(\forall x \in D) P(x)]$ é equivalente a $(\exists x \in D) \neg P(x)$
- $\neg[(\exists x \in D) P(x)]$ é equivalente a $(\forall x \in D) \neg P(x)$

Ou seja, podemos trocar as posições do operador de negação e do quantificador, *desde que também troquemos o tipo de quantificador* (\forall por \exists , e vice-versa). Ressaltamos que estas equivalências valem para qualquer predicado P e qualquer domínio D , e, naturalmente, qualquer que seja a variável usada nos quantificadores.

Por exemplo, considere a afirmação $(\forall n \in \mathbb{N}) n + 1 > 2$. O valor lógico dessa afirmação é falso, pois a proposição aberta “ $n + 1 > 2$ ” não vale quando $n = 0$ ($(0 + 1) = 1$ e 1 não é maior que 2). Por outro lado, este mesmo exemplo mostra que existe um n tal que a afirmação contrária “ $n + 1 \leq 2$ ” é verdadeira; isto é, que $(\exists n \in \mathbb{N}) n + 1 \leq 2$ é verdadeira.

Lembramos que \forall , de certa forma, representa várias conjunções (\wedge); no mesmo sentido que \exists representa várias disjunções (\vee). Observe portanto que as regras para disjunção de quantificadores são análogas às leis de De Morgan para negação de \wedge e \vee .

Estas regras valem também quando o domínio D é vazio. Aliás, a principal justificativa para a regra da seção 3.6.4 é justamente fazer com que as regras de negação de quantificadores sejam válidas em todos os casos. Por exemplo, considere a afirmação “existe um estudante com mais de duzentos anos de idade que não gosta de física”, ou seja $(\exists x \in D) \neg P(x)$ onde D é o conjunto (vazio) dos “estudantes com mais de duzentos anos”, e $P(x)$ é a frase “ x gosta de física”. Esta afirmação é obviamente falsa; e portanto sua negação, $\neg((\exists x \in D) \neg P(x))$, deveria ser verdadeira. De fato, pelas regras acima, a negação desta frase $\neg((\exists x \in D) \neg P(x))$ é $(\forall x \in D) \neg \neg P(x)$, ou seja $(\forall x \in D) P(x)$; e, conforme definimos na seção 3.6.4, esta afirmação tem valor lógico verdadeiro.

3.6.7 Distributividade de quantificadores

Em alguns casos, é possível trocar a ordem de quantificadores com outros conectivos lógicos. Por exemplo, lembrando que \forall representa uma série de conjunções \wedge , e que \exists representa uma série de

disjunções \vee , podemos concluir que

- $(\forall x \in D) (P(x) \wedge Q(x))$ equivale a $((\forall x \in D) P(x)) \wedge ((\forall x \in D) Q(x))$.
- $(\exists x \in D) (P(x) \vee Q(x))$ equivale a $((\exists x \in D) P(x)) \vee ((\exists x \in D) Q(x))$.

3.6.8 Traduzindo linguagem natural para proposições quantificadas

A codificação de proposições da linguagem natural em fórmulas com quantificadores nem sempre é fácil. Na linguagem natural, muitas vezes os quantificadores e/ou o domínio estão implícitos.

Por exemplo, considere a seguinte afirmação: “macacos gostam de bananas.” Nesta afirmação, há um quantificador universal implícito: “*todos* os macacos gostam de bananas.” Sua formalização é portanto $(\forall x \in M) B(x)$ onde M é o conjunto dos macacos, e $B(x)$ é o predicado “ x gosta de banana.”

Outro exemplo é a afirmação “existe um x tal que $x^2 = 5$ ”. O valor lógico dessa afirmação depende do domínio; se escrevermos $(\exists x \in \mathbb{N}) x^2 = 5$, a afirmação é falsa; se escrevermos $(\exists x \in \mathbb{R}) x^2 = 5$, ela é verdadeira. Neste caso, o domínio correto só pode ser determinado pelo contexto da afirmação.

Várias expressões podem ser usadas na língua portuguesa para expressar os quantificadores:

- “para qualquer x em D , $P(x)$ ”,
- “se x é um elemento genérico de D , então $P(x)$ ”,
- “um elemento que está em D sempre satisfaz $P(x)$ ”,
- “para quem está em D , vale $P(x)$ ”,
- “algum elemento de D satisfaz $P(x)$ ”,
- “há elementos em D para os quais $P(x)$ vale”.

Há também muitas expressões para a negação dos quantificadores:

- “nenhum x em D satisfaz $P(x)$ ”,
- “nem todo x em D satisfaz $P(x)$ ”,
- “não há elemento x em D que satisfaça $P(x)$ ”,
- “ninguém em D satisfaz $P(x)$ ”,
- “para nenhum x em D vale $P(x)$ ”,
- “quando x está em D , a afirmação $P(x)$ nem sempre é verdadeira.”

Na linguagem natural, muitas vezes o quantificador está no meio ou no fim da sentença:

- “ $P(x)$ vale para todo x em D ”,

- “ $P(x)$ é verdade para algum x em D ”,
- “ $P(x)$ vale sempre que x está em D ”,
- “ $P(x)$ não é verdade para alguns elementos x de D ”.

Uma maneira de verificar se uma fórmula com quantificadores representa corretamente uma afirmação em linguagem natural é trocar os quantificadores por meio das regras de negação, traduzir o resultado novamente para a linguagem natural, e conferir se o sentido é o mesmo que o original. Por exemplo, suponha que representemos a frase “nenhum gorila é bonito” por $\neg(\exists x \in F) B(x)$, onde F é o conjunto de gorilas, e $B(x)$ significa “ x é bonito”. Pelas regras de negação, esta frase é equivalente a $(\forall x \in F) \neg B(x)$, ou seja, “todos os gorilas são feios”.

É preciso tomar cuidado com certas frases em língua natural cujo sentido é ambíguo. Por exemplo, “em elemento x de D satisfaz $P(x)$ ” pode significar tanto $(\forall x \in D) P(x)$ quanto $(\exists x \in D) P(x)$.

Exercício 3.36: Escreva as afirmações abaixo na forma simbólica, definindo os predicados e os domínios dos quantificadores.

- Todo triângulo equilátero é equiângulo.
- Todos os estudantes gostam de física.
- Alguns estudantes não gostam de física.
- Cada pessoa tem uma mãe.
- Pelo menos uma das letras da palavra *banana* é uma vogal.
- Entre todos os inteiros existem alguns que são primos.
- Um dia do próximo mês é domingo.
- Alguns inteiros são pares e divisíveis por 3.
- Alguns inteiros são pares ou divisíveis por 3.
- $x^2 - 14 = 0$ tem uma solução positiva.
- Toda solução de $x^2 - 14 = 0$ é positiva.
- Nenhuma solução de $x^2 - 14 = 0$ é positiva.
- Existe algum estudante de direito que não é brasileiro.
- Todo estudante de direito tem um celular.
- Ninguém é perfeito.
- Alguém é perfeito.
- Todos os nossos amigos são perfeitos.
- Algun de nossos amigos é perfeito.
- Todos são nossos amigos e são perfeitos.
- Ninguém é nosso amigo ou alguém não é perfeito.
- Apenas um de nossos amigos é perfeito.

Exercício 3.37: Expresse, em português, a negação de cada uma das proposições do exercício 3.36.

Exercício 3.38: Expresse a negação de cada uma das proposições do exercício 3.34 em forma simbólica e em linguagem natural (português).

3.6.9 Mudança de domínio

A regra abaixo permite restringir o domínio das quantificações universais:

- As afirmações $D \subseteq E$ e $(\forall x \in E) P(x)$ implicam logicamente $(\forall x \in D) P(x)$.

Ou seja, uma quantificação universal verdadeira continua verdadeira se restringirmos o domínio a qualquer subconjunto do mesmo. Por exemplo, se sabemos que “todo ruminante tem quatro patas”, e que as zebras são um subconjunto dos ruminantes, podemos concluir que “todas as zebras tem quatro patas”.

Reciprocamente, a regra abaixo permite ampliar o domínio de quantificações existenciais:

- As afirmações $D \subseteq E$ e $(\exists x \in D) P(x)$ implicam logicamente $(\exists x \in E) P(x)$.

Ou seja, uma quantificação existencial verdadeira continua verdadeira se ampliarmos o domínio. Por exemplo, se sabemos que “existe um boi preto”, e que os bois são um subconjunto dos ruminantes, podemos concluir que “existe um ruminante preto”.

Outras regras permitem mudar o domínio no sentido contrário, com ressalvas na fórmula quantificada:

- Se $D \subseteq E$, a afirmação $(\forall x \in D) P(x)$ é logicamente equivalente a $(\forall x \in E) (x \in D \rightarrow P(x))$.
- Se $D \subseteq E$, a afirmação $(\exists x \in D) P(x)$ é logicamente equivalente a $(\exists x \in E) (x \in D \wedge P(x))$.

Por exemplo, se aceitarmos que os papagaios são um subconjunto dos animais, a afirmação “todo papagaio tem um bico” equivale a dizer “todo animal, se for um papagaio, tem um bico;” E a afirmação “existe um papagaio amarelo” equivale a dizer que “existe um animal que é papagaio e é amarelo.”

Um erro comum é confundir as duas regras, e mudar o domínio do quantificador universal com \wedge ao invés de \rightarrow . Por exemplo, traduzir a afirmação “todo macaco gosta de banana” pela fórmula $(\forall x \in A) (x \in M) \wedge B(x)$, onde A é o conjunto dos animais, M é o conjunto dos macacos, e $B(x)$ significa “ x gosta de banana”. Esta fórmula na verdade significa “todo animal é macaco e gosta de banana”, que é bem diferente do sentido original. A fórmula correta seria $(\forall x \in A) (x \in M) \rightarrow B(x)$, que, pelas regras acima, equivale a $(\forall x \in M) B(x)$.

O erro simétrico é usar \rightarrow ao mudar o domínio do quantificador existencial. Por exemplo, representar a afirmação (falsa) “existe um macaco que voa” por $(\exists x \in A) (x \in M) \rightarrow V(x)$, onde A são os animais, M os macacos, e $V(x)$ significa “ x voa”. Esta fórmula na verdade significa “existe um animal que, se for macaco, voa”. Esta afirmação é verdadeira, pois basta considerar um x em $A \setminus M$ (um animal que não é macaco) e a frase $(x \in M) \rightarrow V(x)$ fica $\mathbf{F} \rightarrow V(x)$ e portanto verdadeira. A fórmula correta seria $(\exists x \in A) (x \in M) \wedge V(x)$, que é falsa como a original.

Exercício 3.39: Em cada um dos casos abaixo, procure determinar se as duas proposições são logicamente equivalentes:

- $((\forall x \in A) P(x)) \wedge ((\forall x \in B) P(x))$ equivale a $(\forall x \in A \cup B) P(x)$?
- $((\exists x \in A) P(x)) \vee ((\exists x \in B) Q(x))$ equivale a $(\exists x \in A \cup B) (P(x) \vee Q(x))$?
- $((\forall x \in A) P(x)) \vee ((\forall x \in B) P(x))$ equivale a $(\forall x \in A \cup B) P(x)$?
- $((\exists x \in A) P(x)) \wedge ((\exists x \in B) Q(x))$ equivale a $(\exists x \in A \cup B) (P(x) \vee Q(x))$?

3.6.10 Quantificadores múltiplos

Se uma proposição aberta menciona mais de uma variável, é preciso mais de um quantificador — um para cada variável distinta — para transformá-la numa proposição fechada. Por exemplo, se escolhermos \mathbb{Z} como o domínio, há oito maneiras de transformar a afirmação aberta “ $x + y = 2x$ ” em uma proposição fechada:

$$\begin{aligned} (\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z}) x + y = 2x & \quad (\forall y \in \mathbb{Z})(\forall x \in \mathbb{Z}) x + y = 2x \\ (\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}) x + y = 2x & \quad (\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z}) x + y = 2x \\ (\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z}) x + y = 2x & \quad (\forall y \in \mathbb{Z})(\exists x \in \mathbb{Z}) x + y = 2x \\ (\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z}) x + y = 2x & \quad (\exists y \in \mathbb{Z})(\exists x \in \mathbb{Z}) x + y = 2x \end{aligned}$$

A ordem dos quantificadores pode ser muito importante. Por exemplo, a fórmula $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}) x + y = 2x$ significa “para todo inteiro x , existe um inteiro y (que pode ser diferente para cada x !) tal que $x + y = 2x$ ”. Esta afirmação é verdadeira, pois, para cada x , basta tomar $y = x$ para satisfazer a condição. Por outro lado, a fórmula $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z}) x + y = 2x$ significa “existe um inteiro y tal que, para todo inteiro x (e esse mesmo y !), $x + y = 2x$ ”. Esta frase é falsa, pois, como $x + y = 2x$ é o mesmo que $y = x$, ela equivale a dizer que “existe um inteiro y que é igual a todos os inteiros”.

De modo geral, sempre podemos trocar a ordem de dois quantificadores do mesmo tipo (ambos \forall , ou ambos \exists). Ou seja, para quaisquer variáveis, domínios e predicados,

- A fórmula $(\forall x \in D)(\forall y \in E) P(x, y)$ é logicamente equivalente a $(\forall y \in E)(\forall x \in D) P(x, y)$
- A fórmula $(\exists x \in D)(\exists y \in E) P(x, y)$ é logicamente equivalente a $(\exists y \in E)(\exists x \in D) P(x, y)$

Quando um quantificador sobre uma variável é aplicado a uma proposição aberta que depende dessa variável, dizemos que cada ocorrência dessa variável na proposição está *amarrada* ao quantificador. Todas as demais variáveis que ocorrem na proposição continuam *livres*. Por exemplo, na fórmula $(\forall x \in \mathbb{R}) x^2 + x - y > z/(x + y)$, as três ocorrências de x em $x^2 + x - y > z/(x + y)$ estão amarradas, enquanto que as duas ocorrências de y e a ocorrência de z estão livres.

Enquanto houver variáveis livres, a fórmula continua sendo uma proposição aberta. A fórmula só é uma proposição fechada quando todas as variáveis estiverem amarradas.

Por influência da linguagem natural, alguns autores às vezes escrevem o símbolo quantificador (especialmente ‘ \forall ’) *depois* da fórmula lógica quantificada, como por exemplo em “ $P(x), \forall x \in D$.” Entretanto, este estilo deve ser evitado, pois pode gerar ambiguidade — especialmente quando há vários quantificadores envolvidos. Considere, por exemplo “ $(\exists x \in \mathbb{Z}) x + y = 0, \forall y \in \mathbb{Z}$.”

Exercício 3.40: Sejam \mathbb{N} o conjunto dos números naturais, $P(x, y)$ é “ $x + 2 > y$ ”. Escreva as proposições listadas abaixo em linguagem natural (português) e atribua o valor-verdade correspondente a cada uma delas:

- $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N}) P(x, y)$.
- $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N}) P(x, y)$.
- $(\forall y \in \mathbb{N})(\exists x \in \mathbb{N}) P(x, y)$.

Exercício 3.41: Determine o valor verdade de cada uma das proposições:

- a) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 < m)$.
 b) $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n < m^2)$.
 c) $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(nm = m)$.
 d) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 0)$.
 e) $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n \cdot m = m)$.
 f) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 + m^2 = 5)$.
 g) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n^2 + m^2 = 25)$.
 h) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 4 \wedge n - m = 1)$.
 i) $(\exists n \in \mathbb{N})(\exists m \in \mathbb{N})(n + m = 4 \wedge n - m = 2)$.
 j) $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\exists p \in \mathbb{N})(p = (n + m)/2)$.
 k) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x^2 = y)$.
 l) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x = y^2)$.
 m) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x \cdot y = 0)$.
 n) $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y \neq y + x)$.
 o) $(\forall x \in \mathbb{R}) x \neq 0 \rightarrow (\exists y \in \mathbb{R})(x \cdot y = 1)$.
 p) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(y \neq 0 \rightarrow (x \cdot y = 1))$.
 q) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 1)$.
 r) $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})(x + 2y = 2 \wedge 2x + 4y = 5)$.
 s) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 2 \wedge 2x - y = 1)$.
 t) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})(z = (x + y)/2)$.

Exercício 3.42: Encontre a negação e o valor-verdade de cada uma das proposições do exercício 3.41.

3.6.11 Escopo de um quantificador

A parte da fórmula onde um quantificador tem efeito é chamada de *escopo* do quantificador. Por convenção, o escopo é toda a parte da fórmula que segue ao quantificador; mas podemos usar parênteses para limitar esse escopo. Por exemplo, na fórmula $((\forall x \in D) P(x)) \wedge ((\exists x \in E) Q(x)) \vee R(x)$, o escopo do primeiro quantificador é apenas $P(x)$, o do segundo quantificador é $Q(x)$, e a fórmula $R(x)$ está fora do escopo de ambos — ou seja, a ocorrência de x em $R(x)$ ainda está livre.

3.6.12 Omissão do domínio

O domínio da quantificação pode ser omitido em dois casos. Em primeiro lugar, se, em algum contexto, todos os quantificadores tiverem o mesmo domínio D , podemos anunciar esse fato no início, e escrever apenas $(\forall x) P(x)$ ou $(\exists x) P(x)$, em vez de $(\forall x \in D) P(x)$ ou $(\exists x \in D) P(x)$.

Exercício 3.43: Escreva, em português, as seguintes proposições, supondo que $R(x)$ significa “ x é um rato,” $Q(x)$ significa “ x come queijo,” e o domínio consiste de todos os animais.

- a) $(\forall x) R(x) \rightarrow Q(x)$.

b) $(\forall x)R(x) \wedge Q(x)$.

a) $(\exists x)R(x) \rightarrow Q(x)$.

b) $(\exists x)R(x) \wedge Q(x)$.

Para evitar a quantificação sobre domínios, alguns autores supõem que existe um *conjunto universal* U cujos elementos são todos os elementos de todos os conjuntos que podem vir a ser usados em quantificadores. Nesse caso, podemos usar as equivalências lógicas da seção 3.6.9 para trocar qualquer domínio D pelo domínio universal U :

- $(\forall x \in D) P(x)$ equivale a $(\forall x \in U) (x \in D) \rightarrow P(x)$.
- $(\exists x \in D) P(x)$ equivale a $(\exists x \in U) (x \in D) \wedge P(x)$.

Com estas transformações, todos os quantificadores passam a ter o mesmo domínio U , que pode ser então omitido. Isto é,

- em vez de $(\forall x \in D) P(x)$, pode-se escrever $(\forall x) (x \in D) \rightarrow P(x)$.
- em vez de $(\exists x \in D) P(x)$, pode-se escrever $(\exists x) (x \in D) \wedge P(x)$.

Entretanto, uma vez que conjuntos podem ser elementos de outros conjuntos, todos os conjuntos — inclusive o próprio conjunto universal U — deveriam ser elementos de U . Mas permitir que um conjunto seja elemento de si mesmo pode levar a fórmulas que não fazem sentido (não são nem verdadeiras nem falsas), como “seja X o conjunto de todos os elementos que não pertencem a X .” Por essa razão, muitos lógicos evitam o conceito de “conjunto universal”, e usam domínios explícitos em todos os quantificadores.

Capítulo 4

Métodos de Prova de Teorema

4.1 Introdução

Como vimos no capítulo 1, demonstrações são instrumentos usados por uma pessoa para convencer outras pessoas (ou a si mesma) de que uma afirmação é verdadeira. Toda demonstração precisa partir de algumas definições e/ou afirmações básicas — chamadas *axiomas* ou *postulados* — que ambas as partes aceitam como verdadeiras, e/ou afirmações que foram previamente demonstradas.

Para ser convincente, uma demonstração somente pode usar afirmações e regras de raciocínio que as duas partes consideram válidas. Em geral, podem ser usadas as equivalências e implicações lógicas vistas nos capítulos anteriores. Podem também ser usadas as regras de manipulação de fórmulas da álgebra e da teoria de conjuntos.

Uma afirmação devidamente demonstrada é chamada de *teorema* (palavra derivada de uma expressão grega que significa “verdade dos Deuses”). Um teorema que é demonstrado apenas para ajudar na prova de um outro teorema é chamado de *lema*. Um *corolário* de um teorema é outro teorema que é consequência do primeiro, e cuja demonstração é relativamente simples.

4.1.1 Definições

Uma demonstração também pode usar *definições* que tenham sido feitas previamente. Uma definição precisa ser *completa*, isto é, deve especificar todas as propriedades que identificam exatamente o conceito definido. Deve ser também *precisa*, de modo que o leitor não tenha dúvidas sobre seu significado. Por convenção, o termo definido é enfatizado por ocasião de sua definição. Por exemplo:

Definição 4.1: Um inteiro n é um *múltiplo* de um inteiro p se, e somente se, existe um inteiro q tal que $n = pq$.

Observe que esta definição não deixa dúvidas: para quaisquer inteiros n e p , ela permite ao leitor decidir se n é ou não múltiplo de p . Por outro lado, ela só vale no domínio dos inteiros. O número π é um múltiplo de $\sqrt{17}$? Esta definição não diz nem que sim, nem que não. Enquanto o conceito de “múltiplo” não for definido para números reais, essa frase não tem sentido: ela não é nem verdadeira nem falsa, e portanto não é uma proposição lógica.

Observe também que, na afirmação que define o conceito, as variáveis n e p são livres, enquanto que q está amarrada no quantificador “existe.” Formalmente, podemos entender esta declaração como a definição de um predicado P (“é múltiplo de”) com dois parâmetros (n e p).

Esta definição pode ser usada em demonstrações como se fosse um axioma, ou seja ela nos autoriza a supor que a afirmação

$$(\forall n, p \in \mathbb{Z}) (n \text{ é um múltiplo de } p) \leftrightarrow ((\exists q \in \mathbb{Z}) n = pq)$$

é verdadeira.

Uma vez que um conceito foi definido, ele pode ser usado em outras definições:

Definição 4.2: Um inteiro p divide um inteiro n (é um divisor de n) se, e somente se, n é múltiplo de p .

Observe o uso do conectivo lógico “se e somente se” (\leftrightarrow) nestas definições. Este conectivo permite ao leitor decidir se uma entidade qualquer do domínio se enquadra *ou não* na definição.

Entretanto, em textos matemáticos e técnicos é comum encontrar definições que usam apenas a palavra “se” quando o autor na verdade quer dizer “se e somente se.” Por exemplo:

Definição 4.3: Um inteiro n é *par* se ele é múltiplo de 2.

Esta definição deve ser entendida como “um inteiro n é par se, e somente se, n é múltiplo de 2.” Eis outro exemplo:

Definição 4.4: Se um inteiro não é par, dizemos que ele é *ímpar*.

Há outros formatos de definição que não usam nem “se” nem “se e somente se”. Por exemplo:

Definição 4.5: Um *número primo* é um número inteiro maior que 1, que não tem nenhum divisor exceto 1 e ele mesmo.

4.1.2 Conjeturas

Uma *conjetura* (ou *conjectura*) é uma afirmação para a qual ainda não existe prova. Em geral, este termo é usado quando se suspeita que a afirmação seja verdadeira. Se uma conjetura é finalmente demonstrada, ela se torna um teorema. Por outro lado, se for encontrada uma demonstração da negação da conjetura, dizemos que a mesma foi *refutada*. Enquanto nenhuma das duas coisas ocorre, diz-se que a conjetura continua *aberta*.

Um exemplo famoso é a *conjetura de Fermat*: “se $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras positivas.” Esta conjetura foi encontrada em um livro que pertenceu ao matemático Pierre de Fermat (1601–1665), que escreveu na margem “tenho uma linda demonstração, mas ela não cabe nesta margem.” Apesar de inúmeros esforços por matemáticos de todo o mundo, a afirmação permaneceu como conjetura por mais de 300 anos. Em 1995, finalmente, o matemático inglês Andrew Wiles publicou uma demonstração com mais de 200 páginas. Hoje a conjetura é conhecida como *o último teorema de Fermat*.

Outro exemplo famoso é a *conjetura das quatro cores*: “todo mapa pode ser pintado com no máximo quatro cores, de modo que países vizinhos tenham cores diferentes.” Esta conjetura foi enunciada em 1852 por Francis Guthrie (1831–1899), mas somente foi provada em 1976 por Kenneth Appel e Wolfgang Haken, utilizando um computador. Em 1994 foi produzida uma prova

simplificada por Paul Seymour, Neil Robertson, Daniel Sanders e Robin Thomas, mas continua sendo impossível demonstrar o teorema sem recorrer a um computador.

Há várias conjecturas famosas que ainda estão abertas. A *conjetura de Goldbach*, formulada pelo matemático alemão Christian Goldbach em 1742, afirma que *todo número inteiro par maior que 2 é a soma de dois números primos*. Testes com computadores mostram que esta afirmação é verdadeira para todos os inteiros pares entre 4 e 4×10^{14} (400 trilhões); mas obviamente estes testes não constituem uma prova.

O monge e matemático francês Marin Mersenne (1585–1648) investigou os números $M_n = 2^n - 1$, onde n é um número primo. Estes números, hoje, são chamados *números de Mersenne*. Ele observou que os números $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, e $M_7 = 127$ são primos; mas o número seguinte, $M_{11} = 2047$, não é primo ($2047 = 23 \times 89$). Depois de verificar mais alguns casos, ele conjecturou que M_n é primo para todo n em $\{2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257\}$. Porém, em 1876 Edouard Lucas (1842–1891) provou que $M_{67} = 2^{67} - 1$ não era primo, e portanto a conjectura de Mersenne era falsa. Entretanto, sua prova não exibia os fatores de M_{67} , apenas provava que eles existiam. Em 1903, Frank Nelson Cole (1861–1926) apresentou uma palestra em uma conferência de matemática, com o título vago *On the Factorisation of Large Numbers*. Sem dizer nada, Cole primeiro escreveu $2^{67} - 1$ no quadro negro, e fez os cálculos à mão, obtendo o valor 147573952589676412927. Na outra metade do quadro, ele escreveu o produto $193707721 \times 761838257287$, e fez a multiplicação à mão, obtendo o mesmo resultado. A platéia aplaudiu de pé. Depois ele contou que levou três anos, trabalhando todos os domingos, para encontrar essa fatoração.

4.2 Métodos de prova

Todo teorema tem muitas demonstrações diferentes. Qual é a melhor é, até certo ponto, uma questão de gosto, e depende de para quem a prova é dirigida. Em geral, quanto mais curta a prova, melhor; mas há outros critérios, como a facilidade de compreensão, a simplicidade dos passos, etc.. De modo geral, quando não sabemos se uma afirmação é verdadeira, nossa primeira preocupação é encontrar uma demonstração que nos convença. Para convencer outras pessoas, entretanto, devemos cuidar para que a demonstração seja, além de correta, também simples, clara e objetiva, tanto quanto possível.

Há vários *métodos de demonstração* (*estilos, estratégias, esquemas, etc.*) que são frequentemente usados em matemática. Em geral, a mesma demonstração pode ser reformulada e rearranjada de modo a se enquadrar em vários esquemas distintos. Dependendo do caso, algumas dessas versões podem ser mais fáceis de encontrar, escrever e entender do que outras. No restante deste capítulo vamos descrever algumas técnicas frequentemente utilizadas em provas.

4.3 Prova de implicações

No decorrer de muitas demonstrações, temos que provar implicações da forma $p \rightarrow q$, isto é *se p é verdadeira, então q também é*. A afirmação p é chamada de *hipótese, premissa* ou *condição*, e a afirmação q é chamada de *tese* ou *conclusão*.

4.3.1 Método direto

No *método direto* de demonstração, supomos que a hipótese p é verdadeira, e usamos uma sequência de proposições que são consequências lógicas das anteriores, até obter a tese q . Esta sequência de passos prova a implicação $p \rightarrow q$. Por exemplo, digamos que é preciso provar a afirmação

Teorema 4.1: Se m e n são pares, então $m + n$ é par.

em um contexto onde m e n são números inteiros. Podemos escrever a seguinte demonstração:

Prova:

1. Suponha que m é par. (Hipótese.)
2. Suponha que n é par. (Hipótese.)
3. Existe um inteiro r tal que $m = 2r$. (Definição de “par”).
4. Existe um inteiro s tal que $n = 2s$. (Definição de “par”).
5. Existem inteiros r e s tais que $m + n = 2r + 2s = 2(r + s)$. (De 3 e 4, por álgebra.)
6. Existe um inteiro t tal que $m + n = 2t$. (De 5, chamando $r + s$ de t .)
7. $m + n$ é par. (Definição de “par”, dada 6. Tese.)

Fim.

Na prática, os passos são escritos de maneira muito abreviada, na suposição que o leitor consegue ler os detalhes nas entrelinhas. Por exemplo, a demonstração acima normalmente seria escrita da seguinte maneira:

Prova:

Suponha que m e n são pares. Por definição de número “par”, existem inteiros r e s tais que $m = 2r$ e $n = 2s$. Logo $m + n = 2r + 2s = 2(r + s)$. Como $r + s$ é inteiro, concluímos que o inteiro $m + n$ é par, pela definição. Isto prova que, se m e n são pares, $m + n$ é par.

Fim.

4.3.2 Método da contrapositiva

No *método da contrapositiva*, para provar a afirmação $p \rightarrow q$, supomos que a negação da tese $\neg q$ é verdadeira, e procuramos uma sequência de deduções lógicas que termina com a negação da hipótese $\neg p$. Esta sequência de passos prova que $(\neg q) \rightarrow (\neg p)$. Como vimos na seção 3.3.2, esta afirmação é logicamente equivalente a $p \rightarrow q$, que portanto também está provada.

Por exemplo, digamos que é necessário provar a afirmação:

Teorema 4.2: Se n^2 é par, então n é par.

Prova:

Suponha que n é ímpar. Pela definição de “ímpar”, existe um inteiro k tal que $n = 2k + 1$. Portanto $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Como $2k^2 + 2k$ é um inteiro, pela definição de “ímpar” concluímos que n^2 é ímpar.

Pela regra da contrapositiva, isto prova que, se n^2 é par, então n é par.

Fim.**4.3.3 Método de redução ao absurdo**

O método de redução ao absurdo (também chamado de *prova indireta* ou *por contradição*), baseia-se na equivalência lógica entre a fórmula $(p \rightarrow q)$ e a fórmula $(p \wedge \neg q) \rightarrow \mathbf{F}$, vista na seção 3.3.2. Neste método, para provar a afirmação $p \rightarrow q$, supomos que tanto a hipótese p quanto a negação da tese $\neg q$ são verdadeiras, e procuramos uma sequência de deduções lógicas que termina com uma contradição (uma afirmação com valor lógico \mathbf{F}). Isto prova a afirmação $(p \wedge \neg q) \rightarrow \mathbf{F}$, e portanto também a afirmação equivalente a $p \rightarrow q$.

Por este método, a afirmação

Teorema 4.3: Se m e n são pares, então $m + n$ é par.

pode ser provada desta maneira:

Prova:

Suponhamos que m e n são pares e $m + n$ é ímpar; vamos mostrar que estas suposições levam a uma contradição.

Pela definição de “par”, existem r e s inteiros tais que $m = 2r$ e $n = 2s$. Pela definição de “ímpar”, existe um inteiro j tal que $m + n = 2j + 1$. Logo $2r + 2s = 2j + 1$, ou seja, $r + s - j = 1/2$. Isto é falso pois $r + s - j$ é um inteiro.

Esta contradição prova que, se m e n são pares, $m + n$ é par.

Fim.**4.3.4 Implicação com tese conjuntiva**

Para provar uma conjunção de duas afirmações $p \wedge q$, basta provar cada uma das afirmações separadamente.

Em particular, para provar uma implicação da forma $p \rightarrow (q \wedge r)$, podemos observar que ela equivale logicamente à afirmação “ $(p \rightarrow q) \wedge (p \rightarrow r)$ ”. Portanto, basta provar cada uma destas duas implicações separadamente. Se usarmos o método direto para provar cada implicação, supomos que p é verdadeira; provamos então q ; e provamos em seguida r .

Por exemplo, considere o teorema abaixo:

Teorema 4.4: Se 6 divide um inteiro n , então 2 divide n e 3 divide n .

Prova:

Se 6 divide n então existe um inteiro k tal que $n = 6k$. Então, $n = 2(3k)$, logo 2 divide n . Temos também que $n = 3(2k)$, logo 3 divide n . Portanto 2 divide n e 3 divide n .

Fim.

Depois de provar a parte $p \rightarrow q$, podemos supor que q também é verdadeira, o que pode facilitar a prova de r . Ou seja, para provar $p \rightarrow (q \wedge r)$, podemos provar “ $p \rightarrow q$ ” e em seguida “ $(p \wedge q) \rightarrow r$ ”.

Essa análise pode ser estendida para tese com três ou mais termos, isto é, $p \rightarrow (q_1 \wedge q_2 \wedge q_3 \cdots \wedge q_n)$ é equivalente a $(p \rightarrow q_1) \wedge (p \rightarrow q_2) \wedge \cdots \wedge (p \rightarrow q_n)$.

4.3.5 Implicação com hipótese disjuntiva

Suponha que é necessário provar uma implicação da forma $(p \vee q) \rightarrow r$, onde a hipótese é uma disjunção de duas afirmações. Pode-se verificar que esta implicação equivale a $(p \rightarrow r) \wedge (q \rightarrow r)$. (Note a troca de ‘ \vee ’ por ‘ \wedge ’.) Portanto, basta provar cada uma destas duas implicações separadamente.

Assim como na seção 4.3.4 podemos estender essa técnica para hipóteses com três ou mais termos. Observamos que $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ equivale a $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$ e se cada uma das implicações for provada pelo método direto, a demonstração consistirá de uma lista de casos:

- Caso 1: Supomos que p_1 vale. Provamos q .
- Caso 2: Supomos que p_2 vale. provamos q .
- ...
- Caso n : Supomos que p_n vale. Provamos q .

Note que os casos não precisam ser mutuamente exclusivos. Por exemplo:

Teorema 4.5: Para quaisquer inteiros m e n , se m for par ou n for par, então mn é par.

Prova:

Sejam m e n inteiros quaisquer. Temos dois casos (não exclusivos):

- Caso 1: m é par. Pela definição, existe um inteiro q tal que $m = 2q$. Nesse caso, $mn = (2q)n = 2(nq)$, e portanto mn é par.
- Caso 2: n é par. pela definição, existe um inteiro r tal que $n = 2r$. Nesse caso $mn = m(2r) = 2(mr)$, e portanto mn é par.

Portanto, se m é par ou n é par, mn é par.

Fim.

4.4 Prova de afirmações “se e somente se”

Outro tipo comum de teorema tem a forma $p \leftrightarrow q$, ou seja, “ p vale se e somente se q vale.”

Para demonstrar este tipo de teorema, podemos usar a equivalência lógica entre as afirmações $p \leftrightarrow q$ e $(p \rightarrow q) \wedge (q \rightarrow p)$. Ou seja, dividimos a demonstração em duas partes: (1) prova que $p \rightarrow q$; (2) prova que $q \rightarrow p$. Por exemplo:

Teorema 4.6: Os inteiros x e y são ambos ímpares se, e somente se, o produto xy é ímpar.

Prova:

Sejam x e y inteiros quaisquer.

- Parte (1): provaremos que, se x e y são ímpares, então xy é ímpar. Se x e y são ímpares, por definição existem inteiros r e s tais que $x = 2r + 1$ e $y = 2s + 1$. Portanto $xy = (2r + 1)(2s + 1) = 2(rs + r + s) + 1$. Como $rs + r + s$ é um inteiro, concluímos que xy é ímpar.
- Parte (2): provaremos que, se xy é ímpar, então x e y são ambos ímpares. Ou seja (pela contrapositiva), que se x é par ou y é par, então xy é par. Temos dois casos (não exclusivos):
 - Caso (a): x é par. Neste caso existe um inteiro r tal que $x = 2r$. Portanto $xy = (2r)y = 2(ry)$. Como ry é inteiro, concluímos que xy é par.
 - Caso (b): y é par. Então existe um inteiro s tal que $y = 2s$. Portanto $xy = x(2s) = 2(xs)$. Como xs é inteiro, concluímos que xy é par.

Fim.

Observe que neste exemplo usamos o método da contrapositiva na segunda parte. Com essa escolha, que é bastante comum, a prova de $p \leftrightarrow q$ passa a ser (1) prova de que $p \rightarrow q$; (2) prova de que $(\neg p) \rightarrow (\neg q)$.

Este método pode ser generalizado para afirmações com três ou mais termos, como $(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \dots \wedge (p_{n-1} \leftrightarrow p_n)$. Observe que esta afirmação significa que, no contexto corrente, todas as afirmações p_1, p_2, \dots, p_n são equivalentes. Esta afirmação é logicamente equivalente a $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$. Por exemplo:

Teorema 4.7: Para todo inteiro n , as seguintes afirmações são equivalentes:

1. n é um número par
2. $n - 1$ é um número ímpar
3. n^2 é um número par.

Prova:

Parte (1): vamos provar que se n é par então $n - 1$ é ímpar. Como n é par, por definição existe um inteiro r tal que $n = 2r$. Logo, $n - 1 = 2r - 1 = 2(r - 1) + 1$. Como $r - 1$ é inteiro, concluímos que $n - 1$ é ímpar.

Parte (2) vamos provar que, se $n - 1$ é ímpar, então n^2 é par. Como $n - 1$ é ímpar, existe um inteiro s tal que $n - 1 = 2s + 1$. Logo $n = (2s + 1) + 1 = 2(s + 1)$, e $n^2 = (2(s + 1))^2 = 2(2(s + 1)^2)$. Como $2(s + 1)^2$ é inteiro, concluímos que n^2 é par. Portanto $n^2 = 4(k + 1)^2 = 2(2(k + 1)^2)$ é par.

Parte (3) vamos provar que, se n^2 é par, então n é par. Esta afirmação é verdadeira pelo teorema 4.2.

Fim.

Exercício 4.1: Prove que as seguintes afirmações são equivalentes:

1. $(\exists x) P(x) \wedge (\forall y) (P(y) \rightarrow y = x)$.
2. $(\exists x)(\forall y) P(y) \leftrightarrow y = x$.
3. $(\exists x) P(x) \wedge (\forall y)(\forall z) ((P(y) \wedge P(z)) \rightarrow y = z)$

Exercício 4.2: Prove que, se x e y são números reais, as seguintes afirmações são equivalentes:

1. x é menor que y .
2. A média aritmética de x e y é maior que x .
3. A média aritmética de x e y é menor que y .

Algumas vezes é possível demonstrar afirmações do tipo $p \leftrightarrow q$ sem dividir as duas implicações. Por exemplo, em alguns casos é possível obter q a partir de p (ou vice-versa) através de uma cadeia de equivalências lógicas. Essa cadeia então é uma prova de que $p \leftrightarrow q$.

Teorema 4.8: Sejam A e B conjuntos. Prove que $(A \subseteq \bar{B}) \leftrightarrow (A \cap B = \emptyset)$.

Prova:

$A \subseteq \bar{B}$ é equivalente a $(\forall x \in A) x \in \bar{B}$; que é equivalente a $(\forall x \in A) x \notin B$. Esta afirmação é equivalente a $(\forall x)(x \in A) \rightarrow (x \notin B)$, que é equivalente a $(\forall x), \neg((x \in A) \wedge (x \in B))$. Pela definição de intersecção, esta afirmação equivale a $A \cap B = \emptyset$.

Fim.

4.5 Prova de quantificador universal

4.5.1 Suspensão do quantificador

Muitos teoremas são afirmações com quantificador universal, da forma $(\forall x \in D) P(x)$. Na demonstração deste tipo de teorema, podemos começar supondo que x é um elemento de D escolhido arbitrariamente, e omitir o quantificador no restante da prova. Se, com essa suposição, conseguirmos provar a afirmação $P(x)$, podemos concluir que o teorema original (com o quantificador) é verdadeiro.

O mesmo método pode ser usado para vários quantificadores universais encaixados. Por exemplo:

Teorema 4.9: Para quaisquer números reais x e y , $(x + y)^2 - (x - y)^2 = 4xy$.

Prova:

Sejam x e y dois números reais quaisquer.

Pelo teorema do binômio, temos $(x + y)^2 = x^2 + 2xy + y^2$, e $(x - y)^2 = x^2 - 2xy + y^2$.

Portanto, $(x + y)^2 - (x - y)^2 = (x^2 + 2xy + y^2) - (x^2 - 2xy + y^2) = 4xy$.

Fim.

Ao usar este método, deve-se tomar cuidado para usar variáveis que não tenham significado já definido anteriormente.

4.5.2 Prova por vacuidade

Lembramos que, se E é o conjunto vazio, a afirmação $(\forall x \in E) Q(x)$ é verdadeira, qualquer que seja o predicado Q . Como vimos na seção 3.6.4 esta afirmação é verdadeira *por vacuidade*.

Exemplo 4.1: Todos os pares primos maiores que dois são quadrados perfeitos.

Esta afirmação é verdadeira por vacuidade pois não existem primos pares maiores que dois.

Uma maneira de provar uma afirmação da forma $(\forall x \in D) P(x)$, para um domínio arbitrário D , é mostrar que ela é equivalente a outra afirmação $(\forall x \in E) Q(x)$, para um certo domínio E e algum predicado Q ; e então mostrar que E é vazio.

Por exemplo, a afirmação $(\forall x \in D) A(x) \rightarrow B(x)$ equivale a $(\forall x \in E) B(x)$ onde $E = \{x \in D : A(x)\}$. Portanto, se mostrarmos que $A(x)$ é falsa para todo x em D , a afirmação $(\forall x \in D) A(x) \rightarrow B(x)$ estará provada por vacuidade — qualquer que seja o predicado B .

Exemplo 4.2: Para todo número inteiro x , se $x^2 = 5$ então x é par.

Esta afirmação pode ser escrita $(\forall x \in D) Q(x) \rightarrow P(x)$ onde $D = \mathbb{Z}$, $Q(x)$ significa “ $x^2 = 5$ ”, e $P(x)$ é “ x é par”. Ela é equivalente a “Para todo número inteiro x cujo quadrado é 5, x é par”, ou seja $(\forall x \in E) P(x)$ onde E é o conjunto dos inteiros cujo quadrado é 5. Como E é vazio, a afirmação é verdadeira por vacuidade.

4.6 Prova de teoremas com o quantificador existencial

Muitos teoremas afirmam a existência de objetos com uma propriedade particular, ou seja, são da forma $(\exists x \in D) P(x)$. Veremos a seguir métodos gerais para demonstrar teoremas deste tipo.

4.6.1 Demonstrações construtivas

Uma maneira comum de provar proposições existenciais é através de uma *demonstração construtiva*, em que se exhibe um elemento específico a do domínio D (explicitamente, ou através de uma construção algorítmica) e prova-se que $P(a)$ é verdadeira, para esse elemento. Por exemplo:

Teorema 4.10: Existem três números inteiros positivos tais que $x^2 + y^2 = z^2$.

Prova:

Sejam $x = 3$, $y = 4$, e $z = 5$. Como $x^2 + y^2 = 3^2 + 4^2 = 25 = 5^2 = z^2$, a afirmação é verdadeira.

Fim.

(Três números x, y, z que satisfazem o teorema 4.10 são chamados de *tripla de inteiros pitagóricos* ou *tripla pitagórica*. Essas triplas correspondem a triângulos retângulos cujos lados tem comprimentos inteiros.)

Naturalmente, este método pode ser usado como parte de uma demonstração mais longa. Por exemplo:

Teorema 4.11: Para todo número natural n , se $2^n - 1$ é primo, então n é primo.

Prova:

Seja n um número natural. Vamos provar a contrapositiva, ou seja, que se n não é um número primo, então $2^n - 1$ não é primo. Se $n = 0$ ou $n = 1$, nenhum dos dois é primo, e a afirmação é trivialmente verdadeira. Suponhamos então que n é maior que 1 e não é primo. Por definição, existem inteiros r e s maiores que 1 e menores que n tais que $n = rs$.

Vamos agora mostrar que existe um inteiro x que é divisor próprio de $2^n - 1$. Seja $x = 2^s - 1$ e $y = 1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}$. Então

$$\begin{aligned} xy &= (2^s - 1)(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^s(1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= (2^s + 2^{2s} + \dots + 2^{rs}) - (1 + 2^s + 2^{2s} + \dots + 2^{(r-1)s}) \\ &= 2^{rs} - 1 \\ &= 2^n - 1. \end{aligned}$$

Uma vez que s é maior que 1 e menor que n , temos que $x = 2^s - 1$ é maior que $2^1 - 1 = 1$ e menor que $2^n - 1$. Ou seja, x é um divisor próprio de $2^n - 1$.

Concluimos portanto $2^n - 1$ não é primo.

Fim.

Observe na demonstração acima, que a existência do divisor próprio de $2^n - 1$ foi provada exibindo um x e provando que ele tem essa propriedade.

Outro exemplo é a seguinte afirmação, conhecida como *teorema do deserto de primos*:

Teorema 4.12: Para todo número inteiro positivo n , existe uma sequência de n números inteiros consecutivos que não são primos.

Prova:

Seja n um inteiro positivo, e seja $x = (n + 1)! + 2$. Observe que

$$2 \text{ divide } x = (n + 1)! + 2, \quad (4.1)$$

$$3 \text{ divide } x + 1 = (n + 1)! + 3, \quad (4.2)$$

$$\dots \quad (4.3)$$

$$n + 1 \text{ divide } x + (n - 1) = (n + 1)! + n + 1. \quad (4.4)$$

Logo todos os inteiros $x + i$ com $0 \leq i < n$ são não primos; e eles formam uma sequência de n inteiros consecutivos.

Fim.

4.6.2 Demonstrações não construtivas

Em alguns casos, é possível demonstrar a existência de um elemento que satisfaz uma dada condição mesmo sem exibir explicitamente tal elemento. Uma demonstração deste tipo é chamada de *demonstração não construtiva*. Por exemplo:

Teorema 4.13: Existem dois números reais irracionais x e y tais que x^y é racional.

Prova:

Sabemos que número $\sqrt{2}$ é irracional. Se $(\sqrt{2})^{\sqrt{2}}$ for racional, a afirmação está satisfeita tomando-se $x = \sqrt{2}$ e $y = \sqrt{2}$. Por outro lado, se $(\sqrt{2})^{\sqrt{2}}$ for irracional, podemos tomar $x = (\sqrt{2})^{\sqrt{2}}$ e $y = \sqrt{2}$. Então $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2$ que é racional.

Fim.

Observe que esta demonstração prova que existem valores de x e y que satisfazem a condição, mas deixa em suspenso o valor de x ($\sqrt{2}$ ou $(\sqrt{2})^{\sqrt{2}}$). Para tornar esta demonstração construtiva, teríamos que determinar se $(\sqrt{2})^{\sqrt{2}}$ é racional ou não; mas este é um problema muito difícil.

Outro exemplo clássico de demonstração não construtiva de existência é o seguinte teorema, atribuído a Euclides (360 AC – 295 AC).

Teorema 4.14: Existem infinitos números primos.

Prova:

Vamos usar o método da demonstração por absurdo. Suponhamos que existem finitos números primos, a saber $2, 3, 5, \dots, p$. Seja n o inteiro $(2 \times 3 \times 5 \times \dots \times p) + 1$. Como n é maior que 1, ele tem algum fator primo r . Observe que n não é divisível por $2, 3, 5, \dots, p$, pois tem resto 1 quando dividido por qualquer desses números. Portanto, r , que é divisor de n , não pode ser nenhum dos primos listados acima. Isso contradiz a suposição de que essa lista contém todos os primos.

Fim.

4.6.3 Provas de existência e unicidade

Lembramos que uma afirmação do tipo $(\exists!x \in D) P(x)$ equivale logicamente a

$$((\exists x \in D) P(x)) \wedge ((\forall x \in D)(\forall y \in D) ((P(x) \wedge P(y)) \rightarrow x = y))$$

Portanto, uma demonstração de existência e unicidade pode ser dividida em duas partes:

- *Existência:* prova-se-se (construtivamente ou não) que existe pelo menos um x em D que satisfaz $P(x)$.
- *Unicidade:* supõe-se que y também é um elemento de D que satisfaz $P(y)$, e prova-se que ele é igual ao x cuja existência foi mostrada na primeira parte.

Teorema 4.15: Para todo número complexo z diferente de zero, existe um único número complexo x tal que $zx = 1$.

Prova:

Seja z um número complexo qualquer, diferente de zero. Por definição, existem a e b em \mathbb{R} tais que $z = a + b\mathbf{i}$, onde \mathbf{i} é um elemento de \mathbb{C} tal que $\mathbf{i}^2 = -1$.

Vamos primeiro mostrar que existe pelo menos um x em \mathbb{C} tal que $zx = 1$. Como z é diferente de zero, pelo menos um dos números a e b é diferente de zero. Isso implica que $a^2 + b^2$ é positivo. Seja então $x = (a - b\mathbf{i})/(a^2 + b^2)$. Temos que

$$\begin{aligned} zx &= (a + b\mathbf{i})((a - b\mathbf{i})/(a^2 + b^2)) \\ &= (a^2 - ab\mathbf{i} + ab\mathbf{i} - b^2\mathbf{i}^2)/(a^2 + b^2) \\ &= (a^2 + b^2)/(a^2 + b^2) \\ &= 1. \end{aligned}$$

Suponha agora que y é um número complexo qualquer tal que $zy = 1$; vamos mostrar que ele é igual a x . Multiplicando os dois lados da equação $zy = 1$ por x temos $(zy)x = x$. Como a multiplicação de números complexos é associativa e comutativa, esta afirmação equivale a $(zx)y = x$. Como $zx = 1$, concluímos que $y = x$.

Fim.

4.6.4 Prova de falsidade por contra-exemplo

Demonstrações de existência são usadas, em particular, para refutar conjeturas da forma $(\forall x \in D) P(x)$; pois a negação desta afirmação é $(\exists x \in D) \neg P(x)$. Neste caso dizemos que o elemento x de D que comprovadamente não satisfaz $P(x)$, e que portanto mostra a falsidade da conjetura, é um *contra-exemplo* para a mesma.

Teorema 4.16: Para todo primo n , o inteiro $2^n - 1$ é primo.

Prova:

O número $n = 11$ é um contra-exemplo, pois $P(11) = 2^{11} - 1 = 2047 = 23 \times 89$.

Fim.

Exercício 4.3: Prove (por meio de contra-exemplos) que as seguintes conjeturas são falsas:

- Todo inteiro positivo é soma dos quadrados de três inteiros.

- b) Se n é um número inteiro e $4n$ é par, então n é par.
 c) O produto de dois números irracionais é um número irracional.

Exercício 4.4: Em cada caso abaixo, prove (por meio de contra-exemplo) que as duas proposições não são equivalentes:

- a) $(\forall x \in D) P(x) \vee Q(x)$ e $((\forall x \in D) P(x)) \vee ((\forall x \in D) Q(x))$.
 b) $(\exists x \in D) P(x) \wedge Q(x)$ e $((\exists x \in D) P(x)) \wedge ((\exists x \in D) Q(x))$.

4.7 Exercícios

Prove os seguintes teoremas:

Exercício 4.5: Para todos os números reais a e b , se $a < b$ e $b < 0$ então $a^2 > b^2$.

Exercício 4.6: O quadrado de um número inteiro, não divisível por 5, tem resto 1 ou 4 quando dividido por 5.

Exercício 4.7: Sejam x, y, z números reais. Pelo menos um deles é maior ou igual à média aritmética dos três.

Exercício 4.8: Um inteiro positivo n é par se, e somente se $7n + 4$ é par.

Exercício 4.9: Um número inteiro positivo n é ímpar se, e somente se, $5n + 6$ é ímpar.

Exercício 4.10: Se p é um inteiro ímpar, então a equação $x^2 + x - p = 0$ não tem solução inteira.

Exercício 4.11: Se n é um número inteiro não divisível por 3, então seu quadrado tem resto 1 quando divisível por 3.

Exercício 4.12: Para quaisquer conjuntos A, B, C e D , as seguintes afirmações são sempre verdadeiras

- Se $x \in A$, $(A - B) \subseteq (C \cap D)$ e $x \notin D$, então $x \in B$.
- Se B e C são disjuntos, $A \subseteq C$ e $x \in A$, então $x \notin B$.
- Se $x \in C$ e $(A \cap C) \subseteq B$, então $x \notin (A - B)$.

Exercício 4.13: Não existem soluções inteiras x e y para a equação $x^2 + 3y^2 = 8$.

Exercício 4.14: Existem 100 inteiros consecutivos que não são quadrados perfeitos.

Exercício 4.15: Seja um número inteiro p da forma $4k + 3$, $k \geq 0$. Então não existem inteiros x, y tais que $p = x^2 + y^2$.

Exercício 4.16: Para todo inteiro n , se n não é divisível por 2 ou por 3, então $n^2 - 1$ é divisível por 24.

Exercício 4.17: Se n é um inteiro não divisível por 3, então n^2 dividido por 3 tem resto 1.

Exercício 4.18: Todo inteiro divisível por 2 e por 3 é divisível por 6.

Exercício 4.19: O algarismo das unidades do quadrado de qualquer inteiro n é 0, 1, 4, 5, 6 ou 9.

Exercício 4.20: O algarismo das unidades da quarta potência de qualquer inteiro n é 0, 1, 5 ou 6.

Exercício 4.21: O número $\sqrt{2}$ é irracional.

Exercício 4.22: Se r é um número irracional, então existe um único inteiro n tal que a distância entre r e n é menor do que $1/2$.

Exercício 4.23: Se r é um número irracional, então $\frac{1}{r}$ é irracional.

Exercício 4.24: Se x e y são números reais, então $\max(x, y) + \min(x, y) = x + y$

Exercício 4.25: Se m e n são inteiros ímpares e $m \neq n$, então existe um único inteiro r tal que $|m - r| = |n - r|$

Exercício 4.26: Existem dois inteiros consecutivos, tal que um é um quadrado perfeito e o outro é um cubo perfeito.

Capítulo 5

Indução Matemática

5.1 Introdução

Seja $P(n)$ uma sentença matemática que depende de uma variável natural n , a qual se torna verdadeira ou falsa quando substituímos n por um número natural dado qualquer. Estas sentenças são chamadas *sentenças abertas definidas sobre o conjunto dos números naturais* \mathbb{N} . Exemplos:

1. $P(n)$: “ n é ímpar.” Observe que esta afirmação é verdadeira para alguns valores de n e falsa para outros.
2. $P(n)$: “ $n^2 - n + 41$ é um número primo.” Neste exemplo podemos verificar, não tão facilmente, que $P(1), P(2), \dots, P(40)$ são verdadeiros mas $P(41) = 41^2$ é falso.
3. $P(n)$: “ $2n + 6$ é par.” É fácil ver que $2n + 6 = 2(n + 3)$ para qualquer n , portanto $P(n)$ é verdade para todo n .
4. $P(n)$: “ $1 + 3 + 5 + \dots + (2n + 1) = (n + 1)^2$.” Será que conseguiremos encontrar algum m tal que $P(m)$ seja falso?

Depois de algumas tentativas começamos a desconfiar que a sentença $P(n)$ do exemplo 4 é verdadeira para todo $n \in \mathbb{N}$. Como poderíamos provar isso? Obviamente não podemos testar, um por um, todos os números naturais pois eles são em número infinito. Algumas proposições $P(n)$, como no exemplo 3, podem ser demonstradas usando álgebra e as técnicas estudadas anteriormente. No exemplo 4, como o lado esquerdo da igualdade não é uma forma fechada, ela não pode ser tratada algebricamente. Para estes casos, vamos precisar de uma nova técnica, a *demonstração por indução matemática*.

5.2 Princípio de Indução Matemática

O *princípio da indução matemática* (PIM) é a principal ferramenta para demonstrar sentenças da forma “ $(\forall n \in \mathbb{N}) P(n)$ ”. Ele diz o seguinte:

Axioma 5.1: Seja $P(n)$ uma sentença aberta sobre \mathbb{N} . Suponha que:

1. $P(0)$ é verdade, e
2. Sempre que $P(k)$ é verdade, para algum $k \in \mathbb{N}$, temos que $P(k + 1)$ é verdade.

Então $P(n)$ é verdade para todo $n \in \mathbb{N}$.

Este princípio pode ser visto como uma propriedade fundamental dos números naturais. Estes podem ser definidos por um conjunto de axiomas enunciados pelo matemático Giuseppe Peano em 1889; e um dos postulados de Peano é equivalente ao PIM.

Para demonstrar uma afirmação “ $(\forall n \in \mathbb{N}) P(n)$ ” usando o PIM, podemos então seguir este roteiro:

- *Base da Indução:* Mostrar $P(0)$ é verdade.
- *Hipótese de Indução:* Supor que para algum $k \in \mathbb{N}$, $P(k)$ é verdade.
- *Passo da Indução:* Mostrar que $P(k + 1)$ é verdade.

Exemplo 5.1: Provar que, para todo $n \geq 0$:

$$1 + 3 + 5 + \cdots + (2n + 1) = (n + 1)^2$$

Prova:

- *Base:* $P(0)$ é verdade pois a expressão acima é trivialmente válida para $n = 0$.
- *Hipótese de indução:* suponhamos que para algum k , $P(k)$ é verdade, isto é,

$$1 + 3 + 5 + \cdots + (2k + 1) = (k + 1)^2$$

- *Passo de indução:* temos de provar que $P(k + 1)$ é verdade, isto é temos que mostrar que:

$$1 + 3 + 5 + \cdots + (2k + 1) + (2(k + 1) + 1) = ((k + 1) + 1)^2$$

Pela hipótese de indução, temos

$$[1 + 3 + 5 + \cdots + (2k + 1)] + (2(k + 1) + 1) = [(k + 1)^2] + (2(k + 1) + 1)$$

Por simples álgebra verificamos que o lado direito é igual a

$$((k + 1) + 1)^2$$

Isto mostra que $P(k + 1)$ é verdade, toda vez que $P(k)$ é verdade. Portanto, pelo PIM, a fórmula é válida para todo número natural n .

Fim.

Exemplo 5.2: Dizemos que um conjunto de n retas no plano *estão em posição geral* se não possui duas retas paralelas e nem três retas se interceptando num mesmo ponto. Vamos provar por indução que um conjunto de n retas em posição geral divide o plano em $R_n = n(n+1)/2 + 1$ regiões.

Prova:

- *Base:* Para $n = 0$ temos apenas uma região. Como $R_n = n(n+1)/2 + 1 = 1$, a fórmula é válida neste caso.
- *Hipótese de indução:* Suponhamos que para algum k a fórmula é válida, isto é quaisquer k retas em posição geral dividem o plano em $R_k = k(k+1)/2 + 1$ regiões.
- *Passo da indução:* temos que provar que quaisquer $k+1$ retas em posição geral definem $R_{k+1} = (k+1)(k+2)/2 + 1$ regiões.

Sejam L_1, L_2, \dots, L_{k+1} essas retas. Compare as regiões do plano definidas por elas, que chamaremos de *regiões novas*, com as *regiões velhas* definidas pelas primeiras k dessas retas. Observe que algumas das regiões velhas são divididas pela última reta L_{k+1} , cada uma delas formando duas regiões novas; enquanto que as demais regiões velhas são também regiões novas.

Como as retas estão em posição geral, a reta L_{k+1} cruza cada uma das k retas anteriores em k pontos distintos. Em cada um desses cruzamentos, a reta L_{k+1} passa de uma região velha para outra. Essas regiões são duas a duas distintas porque estão em lados opostos de alguma reta L_i , com $1 \leq i \leq k$. Portanto a reta L_{k+1} corta $k+1$ regiões velhas, que dão origem a $2(k+1)$ regiões novas. Ou seja,

$$R_{k+1} = R_k - (k+1) + 2(k+1) = R_k + (k+1)$$

Como as retas L_1, L_2, \dots, L_k estão em posição geral, podemos usar a hipótese de indução. Obtemos

$$R_k + (k+1) = k(k+1)/2 + 1 + k + 1 = (k+1)(k+2)/2 + 1.$$

Fim.

5.2.1 Formulação do PIM usando conjuntos

O Princípio da Indução Matemática também pode ser enunciando usando a linguagem da teoria de conjuntos:

Teorema 5.1: Seja S um subconjunto de \mathbb{N} tal que

1. $0 \in S$, e
2. Sempre que $k \in S$, para algum $k \in \mathbb{N}$, temos que $k+1 \in S$;

então $S = \mathbb{N}$.

Este teorema pode ser facilmente mostrado usando o PIM. Por outro lado, podemos demonstrar o PIM supondo que o teorema acima é verdade, e considerando o conjunto S de todos os naturais n para os quais $P(n)$ é verdadeira.

Exercício 5.1: Prove que $(\forall n \in \mathbb{N}) 2^0 + 2^{-1} + 2^{-2} + 2^{-3} + \dots + 2^{-n} \leq 2$.

Exercício 5.2: Prove que $(\forall n \in \mathbb{N}) 2^n > n$.

Exercício 5.3: Prove que $(\forall n \in \mathbb{N}) n^n \geq n!$.

Exercício 5.4: Prove que, para todo $n \in \mathbb{N}$, $9^n - 1$ é divisível por 8.

Exercício 5.5: Prove que, para todo $n \in \mathbb{N}$, $a^n - 1$ é divisível por $a - 1$ para todo número inteiro $a > 1$.

Exercício 5.6: Prove que, para todo $n \in \mathbb{N}$, $11^{n+2} + 12^{2n+1}$ é divisível por 133.

Exercício 5.7: Prove que, para todo $n \in \mathbb{N}$, $\frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$ é um número inteiro.

Exercício 5.8: Suponha que uma caixa contém p bolas vermelhas e q bolas amarelas, e que o seguinte procedimento é repetido até sobrar uma única bola na caixa: “Retire duas bolas da caixa; se elas tiverem a mesma cor, coloque uma bola vermelha na caixa; se elas tiverem cores diferentes, coloque uma bola amarela na caixa. Em ambos os casos, não devolva à caixa as bolas retiradas.” Descubra qual é a cor da bola que ficará na caixa. Demonstre por indução que a sua resposta está correta.

5.3 Generalizações da Indução Matemática

Há muitas variações do princípio da indução matemática, que são no fundo equivalentes, mas podem tornar algumas demonstrações mais simples.

5.3.1 Base genérica

Muitas vezes precisamos provar que uma sentença aberta $P(n)$ vale para todos os números naturais maiores ou iguais a um certo n_0 ; ou seja, que “ $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow P(n)$.” Por exemplo, a afirmação $n^2 > 3n$ é verdadeira para todo natural n maior ou igual a 4, embora não seja verdadeira se n for 0, 1, 2 ou 3.

Podemos usar o PIM para provar esse tipo de afirmação, de maneira indireta. Primeiro definimos um outro predicado $Q(m)$ como sendo equivalente a $P(n_0 + m)$. Provamos então a afirmação $(\forall m \in \mathbb{N}) Q(m)$, usando o PIM. Essa afirmação então implica $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow P(n)$.

Este raciocínio justifica o teorema geral abaixo, que nos permite provar tais afirmações por indução matemática de maneira mais direta, usando n_0 como base em vez de 0:

Teorema 5.2: Seja $P(n)$ uma sentença aberta sobre \mathbb{N} . Se

1. $P(n_0)$ é verdadeira, e

2. Para todo $k \geq n_0$, $(P(k) \rightarrow P(k + 1))$.

então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$ com $n \geq n_0$.

Exemplo 5.3: Prove que $n^2 > 3n$ para todo $n \in \mathbb{N}$ com $n \geq 4$.

Prova:

- *Base:* $n = 4$ é verdade pois $16 > 12$.
- *Hipótese de indução:* suponhamos que para algum $k \geq 4$, $k^2 > 3k$.
- *Passo da indução:* provar que $(k + 1)^2 > 3(k + 1)$.

$$(k + 1)^2 = k^2 + 2k + 1$$

Por hipótese de indução $k^2 > 3k$, então

$$k^2 + 2k + 1 > 3k + 2k + 1$$

Como $k \geq 4$ temos que $2k \geq 8$, logo

$$3k + 2k + 1 \geq 3k + 8 + 1 = 3k + 9 = 3(k + 1)$$

portanto, destas duas desigualdades,

$$(k + 1)^2 > 3(k + 1).$$

Fim.

Exercício 5.9: Prove que a soma dos ângulos internos de um polígono convexo de n vértices é $180(n - 2)$.

Exercício 5.10: Prove que o número de diagonais de um polígono convexo de n lados é dado por $d_n = \frac{n(n-3)}{2}$.

Exercício 5.11: Mostre que a soma dos cubos de três números naturais consecutivos é divisível por 9.

Exercício 5.12: Prove que $(\forall n \in \mathbb{N}) n \geq 13 \rightarrow n^2 < (3/2)^n$.

5.3.2 Passo genérico constante

Numa prova por indução, além de começar com uma base n_0 arbitrária, é possível usar um incremento maior que 1 no passo da indução. Ou seja, o passo da indução pode ser a demonstração de que $P(k) \rightarrow P(k + p)$, em vez de $P(k) \rightarrow P(k + 1)$. Nesse caso, o roteiro é dado pelo seguinte teorema geral:

Teorema 5.3: Seja $P(n)$ uma sentença aberta sobre \mathbb{N} , n_0 um número natural qualquer, e p um inteiro positivo. Se

1. $P(n_0), P(n_0 + 1), \dots, P(n_0 + p - 1)$ são verdadeiros, e
2. Para todo $k, k \geq n_0, P(k) \rightarrow P(k + p)$.

então $P(n)$ é verdade para todo $n \geq n_0$.

Observe que, neste caso, a prova da base da indução deve valer para p inteiros consecutivos, $(n_0, n_0 + 1, \dots, n_0 + p - 1)$, e não apenas n_0 .

Exemplo 5.4: Prove que qualquer valor postal inteiro $n \geq 8$ pode ser obtido utilizando apenas selos com valores 3 e 5.

Podemos provar esta afirmação usando o teorema da indução geral 5.3, com incremento $p = 3$:

Prova:

- *Bases:* $n = 8, n = 9, n = 10$. Como $8 = 5 + 3, 9 = 3 + 3 + 3$ e $10 = 5 + 5$ temos que a proposição é válida para as bases.
- *Hipótese de indução:* Suponhamos que $P(k)$ é verdadeira para algum valor $k \geq 8$.
- *Passo:* Vamos mostrar que a proposição é válida para $k + 3$. Podemos obter o valor $k + 3$ acrescentando um selo de valor 3 aos selos usados para obter k .

Fim.

Exercício 5.13: Prove que, para todo valor inteiro $n \geq 5$, em dinheiro, pode ser obtido usando somente notas de 2 ou de 5 reais.

Exercício 5.14: Prove que, para todo inteiro $n \geq 2, \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} \cdots \frac{1}{2n} > \frac{13}{24}$.

Exercício 5.15: Prove que, para todo inteiro $n \geq 3, n^2 - 7n + 12 \geq 0$.

5.4 Mais exemplos de indução matemática

Exemplo 5.5: [Desigualdade de Bernoulli] Se c é um número real tal que $c > -1$ e $c \neq 0$, então para todo número natural $n \geq 2$ vale a desigualdade

$$(1 + c)^n > 1 + nc$$

Prova:

- *Base:* Para $n = 2$ a proposição é verdadeira pois

$$(1 + c)^2 = 1 + 2c + c^2 > 1 + 2c.$$

- *Hipótese de indução:* Para um dado $k \geq 2$, $(1 + c)^k > 1 + kc$
- *Passo:* Mostrar que $(1 + c)^{k+1} > 1 + (k + 1)c$.

Como $(1 + c)^{k+1} = (1 + c)^k(1 + c)$, pela hipótese de indução temos que

$$(1 + c)^{k+1} > (1 + kc)(1 + c) = 1 + (k + 1)c + kc^2 > 1 + (k + 1)c.$$

Logo a desigualdade é válida para $k + 1$. Portanto a desigualdade vale para todo n maior ou igual a 2.

Fim.

Exemplo 5.6: [Conjunto Potência] Seja A um conjunto com n elementos. Mostrar que o conjunto potência $\mathbb{P}(A)$ tem 2^n elementos.

Prova:

- *Base:* Se $n = 0$ temos que o conjunto A é vazio portanto $\mathbb{P}(A) = \{\emptyset\}$, logo o número de elementos de $\mathbb{P}(A)$ é igual a $1 = 2^0$.
- *Hipótese de indução:* Para um dado conjunto A com $k \geq 0$ elementos temos que o conjunto potência $\mathbb{P}(A)$ tem 2^k elementos.
- *Passo:* Mostrar que para um conjunto A com $k + 1$ elementos o conjunto $\mathbb{P}(A)$ tem 2^{k+1} elementos. Seja A um conjunto com $k + 1$ elementos. Como $k \geq 0$, A tem pelo menos um elemento. Seja a este elemento. Considere o conjunto $B = A - \{a\}$. Logo B tem k elementos, o que, pela hipótese de indução, implica que $\mathbb{P}(B)$ tem 2^k elementos. O $\mathbb{P}(A)$ pode ser dividido em dois sub-conjuntos, ou seja

$$\mathbb{P}(A) = \mathbb{P}(B) \cup \{C \cup \{a\} : C \in \mathbb{P}(B)\}.$$

Como $\mathbb{P}(B) \cap \{C \cup \{a\} : C \in \mathbb{P}(B)\} = \emptyset$ e o número de elementos de $|\mathbb{P}(B)| = |\{C \cup \{a\} : C \in \mathbb{P}(B)\}| = 2^k$. concluímos que o número de elementos de $\mathbb{P}(A) = 2^{k+1}$.

Fim.

Exemplo 5.7:[Descobrimo a Moeda Falsa] Num conjunto de 2^n moedas de ouro temos uma que é falsa, ou seja pesa menos que as outras. Mostrar, por indução, que é possível achar a moeda falsa com n pesagens usando uma balança de dois pratos sem usar peso.

Prova:

- *Base:* Para $n = 1$ temos duas moedas e, portanto, basta colocar uma em cada prato para descobrir a falsa.
- *Hipótese de indução:* Usando k pesagens podemos descobrir a moeda falsa dentre 2^k moedas.
- *Passo:* Mostrar que, num conjunto de 2^{k+1} moedas, podemos descobrir a moeda falsa com $k + 1$ pesagens. Divide o conjunto de 2^{k+1} moedas em dois conjuntos de 2^k moedas. Coloca-se esses conjuntos em cada prato da balança. Dessa forma descobrimos em qual conjunto de 2^k moedas se encontra a falsa. Pela hipótese de indução descobre-se a moeda com k pesagens, e, mais a pesagem anterior temos um total de $k + 1$ pesagens.

Fim.

O matemático alemão Johann Dirichlet (1805-1859) enunciou em 1834 o seguinte fato, conhecido como *princípio dos escaninhos* (ou *das gavetas, das casas de pombos* etc.):

Teorema 5.4: Se em n caixas ($n \geq 1$) colocarmos mais de n objetos, então alguma caixa conterá mais de um objeto.

Vamos provar este princípio usando indução matemática no número n de caixas.

Prova:

- *Base:* Para $n = 1$ o resultado é trivial pois, se há mais de um objeto, essa caixa terá mais de um objeto.
- *Hipótese de indução:* Suponhamos que o resultado é válido para algum número $k \geq 1$ de caixas, contendo mais do que k objetos.
- *Passo:* Queremos mostrar que o resultado é válido para $k+1$ caixas contendo mais do que $k+1$ objetos. Seja $m > k+1$ o número de objetos. Escolha uma caixa ao acaso. Se essa caixa contiver mais de um objeto, a proposição está provada. Se nessa caixa não há nenhum objeto, nas k caixas restantes estão acomodados $m > k + 1 > k$ objetos; pela hipótese de indução, uma delas deve conter mais de um objeto. Finalmente, se na caixa escolhida há apenas um objeto, temos que, nas k caixas restantes estão distribuídos $m - 1 > (k + 1) - 1 = k$ objetos, o que, novamente pela hipótese de indução, implica que uma das caixas contém mais de um objeto.

Fim.

5.5 Usos indevidos da indução matemática

É importante entender e verificar as condições em que a indução matemática se aplica. Se mal utilizada, ela pode levar a conclusões absurdas. Nos exemplos a seguir, tente encontrar o erro na demonstração.

Exemplo 5.8: Todos os cavalos tem a mesma cor.

Prova:

Seja a sentença aberta $P(n)$: “Num conjunto com n cavalos, todos os cavalos tem a mesma cor.” Vamos provar que $P(n)$ é verdadeira para todo $n \geq 1$, por indução.

- *Base:* Para $n = 1$ a sentença $P(n)$ é verdadeira.
- *Hipótese de indução:* Suponha que $P(k)$ é verdadeira para algum $k \geq 1$; isto é, em todo conjunto com k cavalos, todos tem a mesma cor.
- *Passo de indução:* Vamos mostrar que, em todo conjunto com $k + 1$ cavalos, todos tem a mesma cor. Considere um conjunto $C = \{c_1, c_2, \dots, c_n, c_{k+1}\}$ com $k + 1$ cavalos. Podemos escrever o conjunto C como união de dois conjuntos, cada um com k cavalos, da seguinte forma:

$$C = C' \cup C'' = \{c_1, \dots, c_k\} \cup \{c_2, \dots, c_{k+1}\}$$

Pela hipótese de indução, todos os cavalos de C' têm a mesma cor. O mesmo é verdade para C'' . Como c_2 pertence a C' e a C'' , concluímos que os cavalos de C' tem a mesma cor que os cavalos de C'' . Logo todos os cavalos de C têm a mesma cor.

Fim.

Este exemplo, conhecido como *paradoxo dos cavalos*, foi inventado pelo matemático húngaro George Pólya (1887-1995). O exemplo a seguir ilustra um erro similar na aplicação do PIM, com “conclusão” igualmente absurda:

Exemplo 5.9: Todos os números naturais são iguais.

Prova:

Seja $P(n)$ a sentença aberta “todos os números naturais menores ou iguais a n são iguais.” Vamos provar que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, por indução.

- *Base:* $P(0)$ é obviamente verdadeira.
- *Hipótese de indução:* Suponha que $P(k)$ é verdadeira para algum $k \geq 0$, ou seja, todos os números menores ou iguais a k são iguais.
- *Passo de indução:* Vamos mostrar que $P(k+1)$ é verdadeira. Pela hipótese de indução, $k - 1 = k$. Somando 1 em ambos os lados da igualdade temos $k = k + 1$. Portanto $P(k + 1)$ também é verdadeira.

Fim.

O próximo exemplo mostra a necessidade de provar a base da indução:

Exemplo 5.10: Para todo número natural $n \geq 1$, o número $n^2 + n$ é ímpar.

Prova:

- *Hipótese de indução:* Suponha que $k^2 + k$ é ímpar para algum $k \geq 1$.
- *Passo de indução:* Vamos mostrar que $(k + 1)^2 + (k + 1)$ é ímpar. Observe que

$$(k + 1)^2 + (k + 1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + 2(k + 1)$$

Este resultado é ímpar, pois $(k^2 + k)$ é ímpar pela hipótese de indução, $2(k + 1)$ é par, e um número ímpar somado com um número par é ímpar.

Fim.

O leitor pode verificar que a afirmação “provada” acima não é verdadeira.

Exercício 5.16: Considere a afirmação (obviamente falsa) $P(n)$: “Para todo número real $a > 0$ e todo natural n , $a^n = 1$ ”. Encontre o erro na demonstração por indução abaixo.

Prova:

- *Base:* $P(0)$ é obviamente verdadeira uma vez que $a^0 = 1$.
- *Hipótese de indução:* Suponha que $P(k)$ é verdadeira para algum $k \geq 0$, ou seja, $a^k = 1$.
- *Passo de indução:* Vamos mostrar que $P(k + 1)$ é verdadeira, isto é $a^{k+1} = 1$. Observe que

$$a^{k+1} = a^{k-1} \cdot a = a^{k-1} \cdot \frac{a^{k-1}}{a^{k-2}} = 1 \cdot \frac{1}{1} = 1.$$

Portanto $P(k + 1)$ também é verdadeira.

Fim.

5.6 Princípio da Indução Completa

Vamos agora enunciar o *princípio da indução completa* (PIC), também chamado de *princípio da indução forte*. Esta versão alternativa do princípio da indução matemática serve, como a anterior, para demonstrar sentenças na forma “ $(\forall n \in \mathbb{N}) P(n)$ ”. Em alguns casos essa técnica torna a demonstração da sentença mais fácil que a técnica anterior. Na seção 5.9 provaremos a equivalência desses dois princípios.

Teorema 5.5: Seja $P(n)$ uma sentença aberta sobre \mathbb{N} . Suponha que

1. $P(0)$ é verdade; e
2. para todo $k \in \mathbb{N}$, $((\forall i \in \mathbb{N}) i \leq k, P(i)) \rightarrow P(k + 1)$,

então $P(n)$ é verdade para todo $n \in \mathbb{N}$.

Portanto para provar que “ $(\forall n \in \mathbb{N}) P(n)$ ” é verdadeiro, usando indução completa, devemos proceder da seguinte forma:

1. *Base da indução:* Mostrar que $P(0)$ é verdade.
2. *Hipótese de indução:* Supor que, para algum $k \in \mathbb{N}$, $P(i)$ é verdade para todo i com $0 \leq i \leq k$.
3. *Passo da indução:* Mostrar que $P(k + 1)$ é verdade.

Como no PIM, podemos generalizar e considerar a base n_0 no lugar de 0.

Exemplo 5.11: Definimos que um número natural $p > 1$ é *primo* quando os únicos divisores dele são 1 e o próprio p . Vamos mostrar que todo inteiro maior ou igual a 2 é primo ou é um produto de primos.

Prova:

Seja $P(n)$ a sentença aberta “ n é primo ou é um produto de primos.” Vamos provar que $(\forall n \in \mathbb{N}) n \geq 2 \rightarrow P(n)$, por indução completa.

- *Base:* $P(2)$ é verdade pois 2 é primo.
- *Hipótese de indução:* Suponha que, para algum $k \geq 2$, $P(i)$ é verdade para todo $i \in \mathbb{N}$ com $2 \leq i \leq k$.
- *Passo da indução:* Vamos provar que $P(k + 1)$ também é verdade. Se $k + 1$ é primo então $P(k + 1)$ é verdadeiro. Se $k + 1$ não é primo, como $k + 1 \geq 2$, ele deve ter algum divisor diferente de 1 e de $k + 1$. Ou seja, $k + 1 = ab$ para algum a e b , com $1 < a \leq k$. Como $a > 1$, concluímos que $b < k + 1$; como $a < k + 1$, concluímos que $b > 1$. Ou seja, $2 \leq a \leq k$ e $2 \leq b \leq k$. Pela hipótese de indução, portanto, a e b são primos ou produtos de primos. Portanto $k + 1 = a \cdot b$ também é um produto de primos.

Fim.

5.6.1 Formulação do PIC usando conjuntos

Assim como no caso do PIM, o princípio da indução completa também pode ser enunciando usando a linguagem da teoria de conjuntos:

Teorema 5.6: Seja S um subconjunto de \mathbb{N} tal que

1. $0 \in S$, e
2. Para todo $k \in \mathbb{N}$, $\{0, 1, 2, \dots, k\} \subseteq S \rightarrow k + 1 \in S$;

então $S = \mathbb{N}$.

5.7 Exercícios

Exercício 5.17: Prove que todo número natural $m > 0$ pode ser escrito como soma de potências de 2, isto é, existem números inteiros n_1, n_2, \dots, n_r , com $0 \leq n_1 < n_2 < \dots < n_r$, tais que

$$m = 2^{n_1} + 2^{n_2} + \dots + 2^{n_r}$$

Exercício 5.18: Sejam m moedas, uma das quais é falsa e tem peso diferente das demais. Use o exercício anterior mostrar, por indução, que bastam n_r pesagens com uma balança de pratos para descobrir a moeda falsa.

Exercício 5.19: Os números de Fibonacci F_0, F_1, F_2, \dots são definidos pelas seguintes regras: $F_0 = 0$, $F_1 = 1$, e $F_n = F_{n-1} + F_{n-2}$ para todo número natural n maior ou igual a 2. Prove, por indução, que

1. $(\forall n \in \mathbb{N}) F_n < (\frac{13}{8})^n$.
2. $(\forall m, n \in \mathbb{N}) F_m F_n + F_{m+1} F_{n+1} = F_{m+n+1}$.
3. $(\forall n \in \mathbb{N}) S_n = F_n - 1$ onde S_n é o número de somas realizadas ao se calcular F_n .

Exercício 5.20: Sejam α e β as duas soluções da equação $x^2 - x - 1 = 0$, com $\alpha > 0$. Prove que $F_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, para todo n em \mathbb{N} .

Exercício 5.21: Sejam x um número real diferente de zero, tal que $x + \frac{1}{x}$ é um número inteiro. Prove que, para todo número natural n , $x^n + \frac{1}{x^n}$ é inteiro.

5.8 Princípio da Boa Ordenação

Uma outra maneira de provar sentenças abertas sobre número naturais é usar uma propriedade dos números naturais conhecida como o *princípio da boa ordenação* (PBO).

Seja S um conjunto de números reais. Um *elemento mínimo* de S é um $y \in S$ tal que para todo $x \in S$, $y \leq x$. O princípio da boa ordenação diz que

Teorema 5.7: Todo subconjunto não vazio S de \mathbb{N} tem um elemento mínimo.

Note que esta afirmação não é válida para subconjuntos de \mathbb{R} ou \mathbb{Z} ; isto é, existem subconjuntos de \mathbb{R} e de \mathbb{Z} que não tem elemento mínimo.

Como exemplo de uso do PBO, vamos provar o *Teorema da Divisão de Euclides*:

Teorema 5.8: Sejam $a, b \in \mathbb{N}$, com $b \neq 0$. Então existem $q, r \in \mathbb{N}$ tais que $a = bq + r$ com $0 \leq r < b$.

Prova:

Sejam $a, b \in \mathbb{N}$, com $b \neq 0$, e seja

$$S = \{a - b \cdot k : k \in \mathbb{N}, a - b \cdot k \geq 0\}$$

Observe que $S \subseteq \mathbb{N}$ pois $a - b \cdot k \geq 0$; e que $S \neq \emptyset$ pois contém $a = a - b \cdot 0$. Então pelo PBO S tem um elemento mínimo. Seja $r = a - b \cdot q$ esse elemento.

Suponha agora que $r \geq b$. Nesse caso $a - b \cdot (q + 1) = r - b \geq 0$, e portanto $r - b$ está também em S . Como $b > 0$, temos $r - b < r$. Isto contraria a escolha de r como o menor elemento de S . Portanto $r < b$.

Fim.

5.9 Formas equivalentes do princípio da indução

Nesta seção vamos provar a equivalência do princípio da indução matemática e do princípio da indução completa. Para isso vamos utilizar o princípio da boa ordenação (PBO). Vamos provar que

$$PIM \rightarrow PBO \rightarrow PIC \rightarrow PIM.$$

5.9.1 PIM implica PBO

Vamos supor que o princípio da indução matemática é válido, e provar o princípio da boa ordenação.

Prova:

Seja S um subconjunto de \mathbb{N} que não possui elemento mínimo; vamos mostrar que ele só pode ser o conjunto vazio. Considere a sentença aberta $P(n)$: “todo elemento de S é maior que n ”. Vamos provar $(\forall n \in \mathbb{N}) P(n)$ por indução matemática.

- *Base:* como $0 \leq x$ para todo $x \in \mathbb{N}$, 0 não pertence a S , pois caso contrário seria um elemento mínimo. Logo, $P(0)$ é verdadeira.
- *Hipótese de indução:* Vamos supor que $P(k)$ é verdadeira para algum k ; isto é, todo elemento de S é maior que k .
- *Passo da indução:* Vamos provar que $P(k + 1)$ é verdadeira. Todo elemento x de S é maior que k , portanto é maior ou igual a $k + 1$. Segue daí que o número $k + 1$ não pode pertencer a S , pois nesse caso seria um elemento mínimo. Portanto, todo elemento de S é maior que $k + 1$. Ou seja, $P(k + 1)$ é verdadeira.

Por outro lado, se x é um elemento qualquer de S , a afirmação $P(x)$ é falsa. Portanto, a afirmação $(\forall n \in \mathbb{N}) P(n)$ implica que S é vazio.

Fim.

5.9.2 PBO implica PIC

Vamos supor agora que o princípio da boa ordenação é válido, e provar o princípio da indução completa.

Prova:

Suponha que $P(n)$ é uma sentença aberta que satisfaz as condições do PIC, isto é

1. $P(0)$ é verdade; e
2. para todo $k \in \mathbb{N}$, $((\forall i \in \mathbb{N}) i \leq k \rightarrow P(i)) \rightarrow P(k + 1)$.

Considere o conjunto $S = \{n \in \mathbb{N} : P(n) \text{ é falsa}\}$. Se S não for vazio, pelo PBO ele possui um elemento mínimo. Pela condição 1 acima, este elemento é positivo, ou seja é $k + 1$ para algum $k \in \mathbb{N}$. Como $k + 1$ é mínimo, $P(i)$ deve ser verdadeira para todo natural $i \leq k$. Mas pela condição 2, $P(k + 1)$ deve ser verdadeira, ou seja $k + 1 \notin S$. Esta contradição significa que S é vazio, ou seja $P(n)$ é verdadeira para todo n .

Fim.

5.9.3 PIC implica PIM

Para concluir, vamos supor que o PIC é verdade, e provar o PIM.

Prova:

Seja $P(n)$ uma sentença aberta que satisfaz as condições do PIM, isto é,

1. $P(0)$ é verdade; e
2. para todo $k \in \mathbb{N}$, $P(k) \rightarrow P(k + 1)$.

A segunda afirmação implica que

- 2'. para todo $k \in \mathbb{N}$, $((\forall i \leq k) P(i)) \rightarrow P(k + 1)$.

Nesta passagem usamos o fato que $(\forall i \leq k) P(i)$ equivale a

$$((\forall i < k) P(i)) \wedge P(k)$$

e o teorema da lógica proposicional (exercício 3.24)

$$(p \rightarrow q) \rightarrow (r \wedge p \rightarrow q)$$

onde $A = P(k)$, $B = P(k + 1)$, e $C = ((\forall i < k) P(i))$ As condições 1 e 2' são as hipóteses do PIC, portanto concluímos que $P(n)$ é verdadeira para todo n .

Fim.

5.10 Exercícios adicionais

Exercício 5.22: Mostre a validade das seguintes fórmulas:

1. $(\forall n \in \mathbb{N}) 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$.
2. $(\forall n \in \mathbb{N}) 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
3. $(\forall n \in \mathbb{N}) 1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$.
4. $(\forall n \in \mathbb{N}) 1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2$.
5. $(\forall n \in \mathbb{N}) 2^0 + 2^1 + 2^2 + \dots + 2^n = 2^{n+1} - 1$.
6. $(\forall n \in \mathbb{N}) 1^2 - 2^2 + 3^2 - \dots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$.
7. $(\forall n \in \mathbb{N}) \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.
8. $(\forall n \in \mathbb{N}) 1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \dots + n \cdot 2^{n-1} = 1 + (n-1)2^n$.

Exercício 5.23: Mostre que as regiões do plano determinadas por n retas, em posição geral, podem ser coloridas utilizando duas cores de modo que regiões adjacentes recebam cores diferentes.

Exercício 5.24: Encontre um inteiro $n_0 \in \mathbb{N}$ que torna as seguintes afirmações verdadeiras, e prove-as por indução em n :

1. $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow 2^n > n^2$.
2. $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n^2 < \left(\frac{5}{4}\right)^n$.
3. $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n! > 2^n$.
4. $(\forall n \in \mathbb{N}) n \geq n_0 \rightarrow n! > 4^n$.

Exercício 5.25: Seja C um conjunto com $n \geq 2$ elementos. Prove, usando indução em n , que C tem $n(n-1)/2$ subconjuntos com exatamente dois elementos.

Exercício 5.26: Mostre, para $n, m \in \mathbb{N}$, que:

$$1 \cdot 2 \dots m + 2 \cdot 3 \dots m(m+1) + \dots + n(n+1) \dots (n+m-1) = \frac{n(n+1) \dots (n+m)}{m+1}$$

Sugestão: Fixe m arbitrário e prove por indução sobre n .

Exercício 5.27: Seja P um polígono no plano. *Triangular* um polígono significa dividir seu interior traçando diagonais que não se cruzam até que todas as regiões obtidas sejam triângulos. Neste caso, dizemos que o polígono P é *triangulado*. Um triângulo T de um polígono triangulado P é *exterior* se dois dos lados de T são lados do polígono P . Na figura 5.1, os triângulos T_1 e T_2 são exteriores.

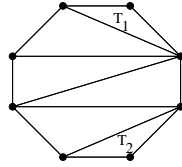


Figura 5.1: Polígono triangulado.

Prove, usando indução matemática, que um polígono triangulado P com quatro ou mais lados possui pelo menos dois triângulos exteriores.

Capítulo 6

Relações

Funções como seno e logaritmo, e os sinais de comparação ‘>’, ‘=’, etc., são casos particulares de *relações*, um conceito fundamental da matemática.

6.1 Conceitos básicos

Uma *relação binária* (ou simplesmente uma *relação*) \mathcal{R} de um conjunto A para um conjunto B é um sub-conjunto de $A \times B$. Em outras palavras, é um conjunto de pares ordenados (a, b) com $a \in A$ e $b \in B$.

Em geral usa-se a notação $a\mathcal{R}b$ para dizer que $(a, b) \in \mathcal{R}$ e $a\not\mathcal{R}b$ para dizer que $(a, b) \notin \mathcal{R}$. Se $(a, b) \in \mathcal{R}$ dizemos que *a está relacionado com b* pela relação \mathcal{R} .

Exemplo 6.1: Sejam $A = \{1, 2, 3\}$, $B = \{4, 5\}$. Então $\mathcal{R} = \{(1, 4), (2, 5), (3, 5)\}$ é uma relação de A para B . Neste exemplo, temos $2\mathcal{R}5$ e $3\mathcal{R}5$, mas $2\not\mathcal{R}4$ e $5\not\mathcal{R}2$.

Se os conjuntos A e B são finitos e suficientemente pequenos, uma relação pode ser representada por um diagrama, em que cada elemento de A ou B é representado por um ponto, e cada par ordenado (a, b) por uma seta de a para b . Veja a figura 6.1.

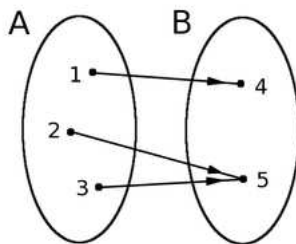


Figura 6.1: Diagrama da relação $\mathcal{R} = \{(1, 4), (2, 5), (3, 5)\}$ do conjunto $A = \{1, 2, 3\}$ para o conjunto $B = \{4, 5\}$.

Exemplo 6.2: Sejam $C = \{1, 2, 3, 4\}$ e $D = \{4, 5, 6\}$. Observe que o conjunto de pares \mathcal{R} do exemplo anterior também é uma relação de C para D .

Exemplo 6.3: O conjunto de pares $\{(x, \sqrt{x}) : x \in \mathbb{N}\}$ é um exemplo de uma relação de \mathbb{N} para \mathbb{R} .

Se R é uma relação de A para A , dizemos que \mathcal{R} é uma relação *em* A ou *sobre* A .

Observe que os sinais de comparação da álgebra (“<”, “≤”, etc.) são relações binárias definidas sobre os números reais.

Observe também que “ \in ” é uma relação binária entre o conjunto \mathcal{U} de todos os elementos, e o conjunto $\mathbb{P}(\mathcal{U})$ de todos os conjuntos; e que “ \subseteq ” é uma relação binária definida sobre o conjunto de todos os conjuntos.

6.1.1 Domínio e imagem

O *domínio* de uma relação \mathcal{R} , denotado por $\text{Dom}(\mathcal{R})$, é o conjunto de todos os primeiros elementos dos pares ordenados que estão em \mathcal{R} . Isto é:

$$\text{Dom}(\mathcal{R}) = \{ a : (a, b) \in \mathcal{R} \}$$

A *imagem* ou *contra-domínio* de uma relação \mathcal{R} , denotado por $\text{Img}(\mathcal{R})$, é o conjunto de todos os segundos elementos dos pares ordenados que estão em \mathcal{R} . Isto é:

$$\text{Img}(\mathcal{R}) = \{ b : (a, b) \in \mathcal{R} \}$$

Observe que um conjunto de pares ordenados \mathcal{R} é uma relação de A para B se, e somente se, $\text{Dom}(\mathcal{R}) \subseteq A$ e $\text{Img}(\mathcal{R}) \subseteq B$.

Exemplo 6.4: Seja \mathcal{R} a relação $\{(1, 4), (2, 5), (3, 5)\}$. Temos que $\text{Dom}(\mathcal{R}) = \{1, 2, 3\}$ e $\text{Img}(\mathcal{R}) = \{4, 5\}$.

Exemplo 6.5: Seja \mathcal{R} a relação $\{(x, x^2) : x \in \mathbb{Z}\}$. Observe que $\text{Dom}(\mathcal{R})$ é o conjunto de todos os inteiros \mathbb{Z} , mas $\text{Img}(\mathcal{R})$ é o conjunto dos quadrados perfeitos $\{0, 1, 4, 9, \dots\}$.

Exemplo 6.6: Seja A o conjunto dos presidentes do Brasil, de 1889 a 2010. Seja \mathcal{R} a relação sobre A tal que $a\mathcal{R}b$ se e somente se o presidente b foi o sucessor de a . Assim, por exemplo, temos que Figueiredo \mathcal{R} Tancredo e Fernando Henrique \mathcal{R} Lula, mas Lula $\not\mathcal{R}$ Fernando Henrique. Observe que o domínio desta relação são todos os presidentes menos Lula (que terminou o mandato em 2010), e a imagem são todos os presidentes menos Floriano Peixoto.

Exemplo 6.7: Seja $A = \{1, 2, 3\}$, e \mathcal{R} o conjunto dos pares (a, b) de $A \times A$ tais que $a < b$. Ou seja, $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$. Neste caso, $\text{Dom}(\mathcal{R}) = \{1, 2\}$ e $\text{Img}(\mathcal{R}) = \{2, 3\}$.

Exemplo 6.8: Seja A o conjunto dos números inteiros e $\mathcal{R} = \{(a, b) : a\mathcal{R}b \leftrightarrow a = 2b\}$. Note que $\text{Dom}(\mathcal{R})$ é o conjunto dos inteiros pares e $\text{Img}(\mathcal{R}) = \mathbb{Z}$.

Exemplo 6.9: Seja A o conjunto dos números reais e $\mathcal{R} = \{(a, b) : a^2 + b^2 = 25\}$. Neste caso $\text{Dom}(\mathcal{R}) = \{a : -5 \leq a \leq 5\}$ e $\text{Img}(\mathcal{R}) = \{b : -5 \leq b \leq 5\}$.

Exercício 6.1: Prove que, para qualquer relação \mathcal{R} , a imagem $\text{Img}(\mathcal{R})$ é vazia se e somente se o domínio $\text{Dom}(\mathcal{R})$ é vazio.

6.1.2 Restrição de relações

Seja \mathcal{R} uma relação, e sejam A' e B' conjuntos quaisquer. A *restrição de \mathcal{R} a A' e B'* é o conjunto de pares de $(a, b) \in \mathcal{R}$ tais que $a \in A'$ e $b \in B'$; ou seja, $\mathcal{R} \cap A' \times B'$. A *restrição de \mathcal{R} a A'* é geralmente entendida como $\mathcal{R} \cap A' \times A'$.

Exemplo 6.10: Seja \mathcal{R} a relação dos inteiros positivos $\mathbb{N} \setminus \{0\}$ para os inteiros, tal que $x\mathcal{R}y$ se e somente se x é divisor de y . A restrição de \mathcal{R} aos conjuntos $U = \{0, 2, 3, 5, 6\}$ e $V = \{0, 1, 2, \dots, 9\}$ é o conjunto de pares

$$\{(2, 0), (2, 2), (2, 4), (2, 6), (2, 8), (3, 0), (3, 6), (3, 9), (5, 0), (5, 5), (6, 0), (6, 6)\}$$

A restrição de \mathcal{R} ao conjunto U é

$$\{(2, 0), (2, 2), (2, 6), (3, 0), (3, 3), (3, 6), (5, 0), (5, 5), (6, 0), (6, 6)\}$$

É comum se usar uma relação \mathcal{R} que foi definida sobre um conjunto A como se fosse uma relação sobre qualquer subconjunto $A' \subset A$, quando na realidade se deveria usar a restrição de \mathcal{R} a A' . Por exemplo, a relação ' \leq ' é definida sobre os reais \mathbb{R} , mas ela é frequentemente usada como se fosse também uma relação sobre os inteiros \mathbb{Z} , os naturais \mathbb{N} , ou qualquer outro subconjunto de \mathbb{R} . Nestes casos entende-se que a relação desejada é a restrição de ' \leq ' a estes subconjuntos.

6.1.3 Relações de identidade

Para qualquer conjunto A , a relação *identidade sobre A* , denotada por \mathcal{I}_A , é definida por

$$\mathcal{I}_A = \{(x, x) : x \in A\}$$

Esta relação nada mais é que a relação de igualdade "=", restrita ao conjunto A .

Exemplo 6.11: Se $A = \{1, 2, 3\}$ então $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$.

6.1.4 Relação inversa

Seja \mathcal{R} uma relação do conjunto A para o conjunto B . A *relação inversa* denotada por \mathcal{R}^{-1} , é a relação do conjunto B para o conjunto A definida da seguinte forma:

$$\mathcal{R}^{-1} = \{(x, y) : (y, x) \in \mathcal{R}\}$$

Ou seja, \mathcal{R}^{-1} é a relação tal que $a\mathcal{R}^{-1}b$ se e somente se $b\mathcal{R}a$, para quaisquer a e b . Observe que $\text{Dom}(\mathcal{R}^{-1}) = \text{Img}(\mathcal{R})$ e $\text{Img}(\mathcal{R}^{-1}) = \text{Dom}(\mathcal{R})$.

Exemplo 6.12: Seja $A = \{1, 2, 3\}$ e \mathcal{R} a relação sobre A do exemplo 6.7. A relação inversa é $\mathcal{R}^{-1} = \{(a, b) : b\mathcal{R}a\} = \{(a, b) : a \in A \wedge b \in A \wedge b < a\} = \{(2, 1), (3, 1), (3, 2)\}$. Veja que $\text{Dom}(\mathcal{R}^{-1}) = \{2, 3\}$ e $\text{Img}(\mathcal{R}^{-1}) = \{1, 2\}$.

Exemplo 6.13: A inversa de " \in ", denotada por " \ni ", é uma relação do conjunto $\mathbb{P}(\mathcal{U})$ de todos os conjuntos para o conjunto \mathcal{U} de todos os elementos. A fórmula $A \ni x$ (lê-se "A possui x ", ou "A tem x ") significa a mesma coisa que $x \in A$. (Note a diferença entre " \ni ", " \supseteq ", e " \supset ".)

Exercício 6.2: Qual é inversa da relação "<"? E da relação "="? E da relação "⊆"?

Exercício 6.3: Se A é um conjunto com m elementos, quantas relações distintas existem sobre A ? Se B é um conjunto com n elementos, quantas relações existem de A para B ?

6.1.5 Imagem e imagem inversa de conjuntos

Definição 6.1: Sejam \mathcal{R} uma relação de um conjunto A para um conjunto B , e X um conjunto qualquer. A *imagem de X sob \mathcal{R}* é o conjunto

$$\{b : (\exists a \in X)(a, b) \in \mathcal{R}\}$$

A *imagem inversa de X sob \mathcal{R}* é o conjunto

$$\{a : (\exists b \in X)(a, b) \in \mathcal{R}\}$$

Observe que a imagem inversa de X sob \mathcal{R} é a imagem de X sob a relação inversa \mathcal{R}^{-1} . A imagem de X sob \mathcal{R} costuma ser indicada por $\mathcal{R}(X)$. A imagem inversa então pode ser indicada por $\mathcal{R}^{-1}(X)$.

6.2 Composição de relações

Sejam \mathcal{R} e \mathcal{S} duas relações. A *composição de \mathcal{R} com \mathcal{S}* é a relação denotada por $\mathcal{S} \circ \mathcal{R}$, e definida da seguinte forma:

$$\mathcal{S} \circ \mathcal{R} = \{(a, c) : (\exists b)(a, b) \in \mathcal{R} \wedge (b, c) \in \mathcal{S}\}$$

Exemplo 6.14: Considere as relações

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

$$\mathcal{S} = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$$

A composição delas é

$$\mathcal{S} \circ \mathcal{R} = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}$$

Observe que

- $(1, 0) \in \mathcal{S} \circ \mathcal{R}$ porque $(1, 1) \in \mathcal{R}$ e $(1, 0) \in \mathcal{S}$,
- $(1, 1) \in \mathcal{S} \circ \mathcal{R}$ porque $(1, 4) \in \mathcal{R}$ e $(4, 1) \in \mathcal{S}$,
- $(2, 1) \in \mathcal{S} \circ \mathcal{R}$ porque $(2, 3) \in \mathcal{R}$ e $(3, 1) \in \mathcal{S}$,
- $(2, 2) \in \mathcal{S} \circ \mathcal{R}$ porque $(2, 3) \in \mathcal{R}$ e $(3, 2) \in \mathcal{S}$,
- $(3, 0) \in \mathcal{S} \circ \mathcal{R}$ porque $(3, 1) \in \mathcal{R}$ e $(1, 0) \in \mathcal{S}$,
- $(3, 1) \in \mathcal{S} \circ \mathcal{R}$ porque $(3, 4) \in \mathcal{R}$ e $(4, 1) \in \mathcal{S}$.

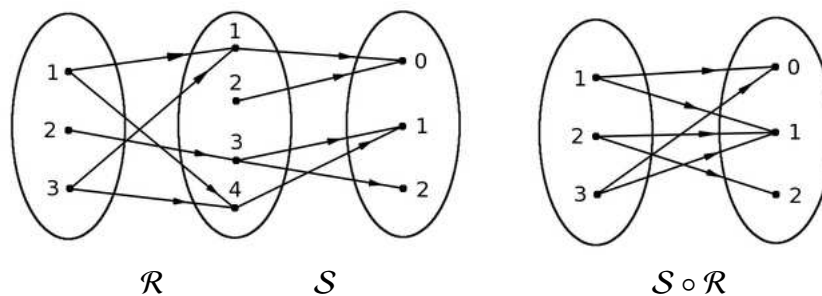


Figura 6.2: Composição das relações do exemplo 6.14.

Exemplo 6.15: Seja \mathcal{R} a relação de \mathbb{Z} para \mathbb{Z} definida por $x\mathcal{R}y \leftrightarrow x = y + 1$. Seja \mathcal{S} a relação de \mathbb{Z} para \mathbb{Z} definida por $y\mathcal{S}z \leftrightarrow y = 2z$. A composição $\mathcal{S} \circ \mathcal{R}$ é a relação de \mathbb{Z} para \mathbb{Z} definida por

$$x(\mathcal{S} \circ \mathcal{R})z \leftrightarrow (\exists y \in \mathbb{Z}) x = y + 1 \wedge y = 2z$$

Ou seja, $x(\mathcal{S} \circ \mathcal{R})z \leftrightarrow x = 2z + 1$. Observe que $(5, 2) \in \mathcal{S} \circ \mathcal{R}$, porque $(5, 4) \in \mathcal{R}$ e $(4, 2) \in \mathcal{S}$. Observe também que $(6, 2) \notin \mathcal{S} \circ \mathcal{R}$, porque o único elemento relacionado com 6 por \mathcal{R} é 5, mas $(5, 2) \notin \mathcal{S}$.

Exemplo 6.16: Sejam \mathcal{R} e \mathcal{S} as mesmas relações do exemplo 6.15. A composição $\mathcal{R} \circ \mathcal{S}$ é a relação de \mathbb{Z} para \mathbb{Z} definida por

$$x(\mathcal{R} \circ \mathcal{S})z \leftrightarrow (\exists y \in \mathbb{Z}) x = 2y \wedge y = z + 1$$

Ou seja, $x(\mathcal{R} \circ \mathcal{S})z \leftrightarrow x = 2z + 2$. Observe que $(5, 2) \notin \mathcal{R} \circ \mathcal{S}$, mas $(6, 2) \in \mathcal{R} \circ \mathcal{S}$.

Os exemplos 6.15 e 6.16 mostram que há casos em que $\mathcal{S} \circ \mathcal{R} \neq \mathcal{R} \circ \mathcal{S}$; isto é, a composição de relações não é comutativa.

Observe que, para quaisquer relações \mathcal{R} e \mathcal{S} , temos

$$\text{Dom}(\mathcal{S} \circ \mathcal{R}) \subseteq \text{Dom}(\mathcal{R})$$

e

$$\text{Img}(\mathcal{S} \circ \mathcal{R}) \subseteq \text{Img}(\mathcal{S})$$

6.2.1 Notação alternativa

A notação $\mathcal{S} \circ \mathcal{R}$ para composição de \mathcal{R} com \mathcal{S} é muito comum, especialmente para funções (vide capítulo 7.1). Em algumas áreas da matemática, entretanto, a composição de uma relação \mathcal{R} com uma relação \mathcal{S} é denotada pela justaposição $\mathcal{R}\mathcal{S}$. Observe que, nesta notação, a ordem das relações é oposta à da notação tradicional.

6.2.2 Composição com identidade

Observe que, para qualquer relação \mathcal{R} de um conjunto A para um conjunto B , as composições $\mathcal{I}_B \circ \mathcal{R}$ e $\mathcal{R} \circ \mathcal{I}_A$ são sempre a própria relação \mathcal{R} .

Exemplo 6.17: Seja $A = \{1, 2, 3\}$, $B = \{10, 20, 30, 40\}$ e $\mathcal{R} = \{(1, 20), (1, 30), (2, 30)\}$. Lembramos que $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$ e $\mathcal{I}_B = \{(10, 10), (20, 20), (30, 30), (40, 40)\}$. Pode-se verificar que $\mathcal{R} \circ \mathcal{I}_A = \mathcal{I}_B \circ \mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$.

6.2.3 Composição com a relação inversa

Considere o seguinte exemplo:

Exemplo 6.18: Seja $A = \{1, 2, 3\}$ e seja $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$, uma relação sobre A . Lembramos que a relação inversa \mathcal{R}^{-1} é $\{(2, 1), (3, 1), (3, 2)\}$, e que $\mathcal{I}_A = \{(1, 1), (2, 2), (3, 3)\}$. Então:

- $\mathcal{R}^{-1} \circ \mathcal{R} = \{(1, 1), (1, 2), (2, 2), (2, 1)\}$.

- $\mathcal{R} \circ \mathcal{R}^{-1} = \{(2, 2), (2, 3), (3, 3), (3, 2)\}$.
- $\mathcal{R} \circ \mathcal{R} = \{(1, 3)\}$.
- $\mathcal{R}^{-1} \circ \mathcal{R}^{-1} = \{(3, 1)\}$.

Observamos que neste exemplo $\mathcal{R} \circ \mathcal{R}^{-1}$ é diferente de $\mathcal{R}^{-1} \circ \mathcal{R}$, e ambas são diferentes da identidade \mathcal{I}_A .

Exercício 6.4: Prove que, para toda relação \mathcal{R} , a composição $\mathcal{R}^{-1} \circ \mathcal{R}$ contém a relação de identidade sobre $\text{Dom}(\mathcal{R})$; e que $\mathcal{R} \circ \mathcal{R}^{-1}$ contém a identidade sobre $\text{Img}(\mathcal{R})$.

6.2.4 Inversa da composição

Pode-se verificar que, para quaisquer relações \mathcal{R} e \mathcal{S} ,

$$(\mathcal{S} \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{S}^{-1}$$

Ou seja, a *inversa da composição é a composição das inversas, na ordem inversa*.

Exemplo 6.19: Sejam as relações

$$\mathcal{R} = \{(1, 20), (1, 30), (2, 40), (3, 20)\}$$

$$\mathcal{S} = \{(20, 200), (20, 300), (40, 200)\}$$

Observe que

- $\mathcal{S} \circ \mathcal{R} = \{(1, 200), (3, 200), (3, 300), (2, 200)\}$.
- $\mathcal{R}^{-1} = \{(20, 1), (30, 1), (40, 2), (20, 3)\}$.
- $\mathcal{S}^{-1} = \{(200, 20), (300, 20), (200, 40)\}$.
- $\mathcal{R}^{-1} \circ \mathcal{S}^{-1} = \{(200, 1), (300, 1), (200, 3), (200, 2), (300, 3)\}$.
- $(\mathcal{S} \circ \mathcal{R})^{-1} = \{(200, 1), (300, 1), (200, 3), (300, 3), (200, 2)\}$.

6.2.5 Composição e inclusão

O seguinte teorema decorre imediatamente das definições:

Teorema 6.1: Para quaisquer relações $\mathcal{R}_1, \mathcal{R}_2, \mathcal{S}_1, \mathcal{S}_2$, se $\mathcal{R}_1 \subseteq \mathcal{R}_2$ e $\mathcal{S}_1 \subseteq \mathcal{S}_2$, então $\mathcal{R}_1 \circ \mathcal{S}_1 \subseteq \mathcal{R}_2 \circ \mathcal{S}_2$.

6.2.6 Potências de uma relação

Seja \mathcal{R} uma relação. A *potência* \mathcal{R}^n , $n = 1, 2, \dots$ é definida como:

$$\begin{aligned} \mathcal{R}^1 &= \mathcal{R} \\ \mathcal{R}^{n+1} &= \mathcal{R}^n \circ \mathcal{R} \end{aligned}$$

Teorema 6.2: Para quaisquer relações \mathcal{R} e \mathcal{S} , e qualquer inteiro $n \geq 1$, se $\mathcal{R} \subseteq \mathcal{S}$ então $\mathcal{R}^n \subseteq \mathcal{S}^n$.

Prova:

Vamos provar este teorema por indução em n .

- *Base:* para $n = 1$, o resultado é verdadeiro, pois $\mathcal{R}^1 = \mathcal{R} \subseteq \mathcal{S} = \mathcal{S}^1$.
- *Hipótese de indução:* vamos supor que, para algum $k \geq 1$, $\mathcal{R}^k \subseteq \mathcal{S}^k$.
- *Hipótese de indução:* vamos provar que $\mathcal{R}^{k+1} \subseteq \mathcal{S}^{k+1}$. Pelo teorema 6.1, concluímos que $\mathcal{R}^k \circ \mathcal{R} \subseteq \mathcal{S}^k \circ \mathcal{S}$. Pela definição de potência, $\mathcal{R}^{k+1} \subseteq \mathcal{S}^{k+1}$.

Fim.

Exercício 6.5: Prove que, se \mathcal{R} é uma relação de A para B , então $\mathcal{R} \circ I_A = I_B \circ \mathcal{R} = \mathcal{R}$.

Exercício 6.6: Prove que, para quaisquer relações \mathcal{R} e \mathcal{S} , vale $\mathcal{R}^{-1} \circ \mathcal{S}^{-1} = (\mathcal{S} \circ \mathcal{R})^{-1}$.

Exercício 6.7: Prove que a composição de relações é associativa; isto é, que, para quaisquer três relações \mathcal{R} , \mathcal{S} e \mathcal{T} , vale $\mathcal{T} \circ (\mathcal{S} \circ \mathcal{R}) = (\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R}$.

Exercício 6.8: Prove que a composição de relações distribui sobre união de relações; isto é, que, para quaisquer três relações \mathcal{R} , \mathcal{S} e \mathcal{T} , vale $\mathcal{T} \circ (\mathcal{R} \cup \mathcal{S}) = (\mathcal{T} \circ \mathcal{R}) \cup (\mathcal{T} \circ \mathcal{S})$, e $(\mathcal{R} \cup \mathcal{S}) \circ \mathcal{T} = (\mathcal{R} \circ \mathcal{T}) \cup (\mathcal{S} \circ \mathcal{T})$.

Exercício 6.9: Prove que para quaisquer três relações \mathcal{R} , \mathcal{S} e \mathcal{T} , vale $\mathcal{T} \circ (\mathcal{R} \cap \mathcal{S}) \subseteq (\mathcal{T} \circ \mathcal{R}) \cap (\mathcal{T} \circ \mathcal{S})$. Encontre um exemplo em que não vale a igualdade; isto é, $\mathcal{T} \circ (\mathcal{R} \cap \mathcal{S}) \neq (\mathcal{T} \circ \mathcal{R}) \cap (\mathcal{T} \circ \mathcal{S})$.

Exercício 6.10: Prove que, para toda relação \mathcal{R} e quaisquer m e n inteiros, $\mathcal{R}^m \circ \mathcal{R}^n = \mathcal{R}^{m+n}$.

6.3 Representação de relações usando matrizes

6.3.1 Matriz booleana de uma relação

Uma *matriz booleana* é uma matriz cujos elementos são valores lógicos, **F** ou **V**. Ao escrever tais matrizes, é conveniente usar 0 e 1, respectivamente, para indicar esses valores.

Sejam $A = \{a_1, a_2, \dots, a_m\}$ e $B = \{b_1, b_2, \dots, b_n\}$ conjuntos finitos com $|A| = m$, $|B| = n$ e \mathcal{R} uma relação de A para B . Uma maneira de representar esta relação é através de uma matriz booleana M de m linhas e n colunas definida da seguinte maneira:

$$M_{i,j} = \begin{cases} 1 & \text{se } a_i \mathcal{R} b_j \\ 0 & \text{se } a_i \not\mathcal{R} b_j \end{cases}$$

Observe que a matriz M depende da escolha dos conjuntos A e B , e também da ordem em que listamos seus elementos.

Exemplo 6.20: Seja \mathcal{R} a relação $\{(20, 20), (30, 20), (30, 30)\}$. Se escolhermos $A = \{10, 20, 30, 40\}$ e $B = \{10, 20, 30\}$, listados nessa ordem, a matriz da relação será

$$M = \left(\begin{array}{c|ccc} & 10 & 20 & 30 \\ \hline 10 & 0 & 0 & 0 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 1 & 1 \\ 40 & 0 & 0 & 0 \end{array} \right)$$

6.3.2 Operações com relações usando matrizes

A representação por matrizes também pode ser usada para visualizar operações entre relações.

União de relações. Sejam \mathcal{R} e \mathcal{S} duas relações de um conjunto A para um conjunto B , com matrizes booleanas M e N , respectivamente. A matriz booleana P que representa a união $\mathcal{R} \cup \mathcal{S}$ é tal que $P_{i,j} = 1$ se, e somente se, $M_{i,j} = 1$ ou $N_{i,j} = 1$. Ou seja, $P_{i,j} = M_{i,j} \vee N_{i,j}$. Podemos denotar essa matriz por $M \vee N$.

Intersecção de relações. Analogamente, a matriz Q que representa a intersecção $\mathcal{R} \cap \mathcal{S}$ é tal que $Q_{i,j} = 1$ se e somente se $M_{i,j} = 1$ e $N_{i,j} = 1$; ou seja $Q_{i,j} = M_{i,j} \wedge N_{i,j}$. tiverem 1 e 0 caso contrário. Podemos denotar essa matriz por $M \wedge N$.

Exemplo 6.21: Sejam $A = \{10, 20, 30, 40\}$ e $B = \{20, 40, 60\}$, e sejam

$$\mathcal{R} = \{(10, 20), (10, 60), (20, 40), (40, 60)\}$$

$$\mathcal{S} = \{(10, 20), (20, 60), (30, 40), (40, 20)\}$$

As matrizes booleanas que representam \mathcal{R} , \mathcal{S} , $\mathcal{R} \cup \mathcal{S}$ e $\mathcal{R} \cap \mathcal{S}$ são

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array} \right) \quad N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 0 \\ 20 & 0 & 0 & 1 \\ 30 & 0 & 1 & 0 \\ 40 & 1 & 0 & 0 \end{array} \right)$$

$$M \vee N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 1 \\ 30 & 0 & 1 & 0 \\ 40 & 1 & 0 & 1 \end{array} \right) \quad M \wedge N = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 0 \\ 20 & 0 & 0 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 0 \end{array} \right)$$

Composição de relações. A composição de relações também pode ser entendida em termos de matrizes. Sejam \mathcal{R} uma relação de $A = \{a_1, a_2, \dots, a_m\}$ para $B = \{b_1, b_2, \dots, b_n\}$, e \mathcal{S} uma relação de B para $C = \{c_1, c_2, \dots, c_p\}$, com matrizes booleanas M ($m \times n$) e N ($n \times p$), respectivamente. Pela definição, a matriz P que representa a composição $\mathcal{S} \circ \mathcal{R}$ é tal que $P_{i,j} = 1$ se e somente se existe um inteiro $k \in \{1, 2, \dots, n\}$ tal que $M_{i,k} = 1$ e $N_{k,j} = 1$. Ou seja,

$$P_{i,j} = (M_{i,1} \wedge N_{1,j}) \vee (M_{i,2} \wedge N_{2,j}) \vee \dots \vee (M_{i,n} \wedge N_{n,j})$$

que pode ser escrita mais sucintamente como

$$P_{i,j} = \bigvee_{k=1}^n M_{i,k} \wedge N_{k,j}$$

(Veja o capítulo 8.8.) Note a semelhança entre esta fórmula e a fórmula do produto de duas matrizes ordinárias,

$$P_{i,j} = \sum_{k=1}^n M_{i,k} \cdot N_{k,j}$$

Concluimos que a composição de uma relação \mathcal{R} com uma relação \mathcal{S} corresponde ao produto MN das respectivas matrizes booleanas M e N , no sentido da álgebra de matrizes; exceto que o produto “ \cdot ” de dois números é substituído pela conjunção “ \wedge ”, e a soma de números “ $+$ ” é substituída pela disjunção “ \vee ”. Observe que a ordem em que as matrizes devem ser multiplicadas é oposta à ordem usada na notação $\mathcal{S} \circ \mathcal{R}$.

Exemplo 6.22: Sejam $A = \{10, 20, 30, 40\}$, $B = \{20, 40, 60\}$, e $C = \{35, 55, 75, 95\}$. Sejam

$$\mathcal{R} = \{(10, 20), (10, 60), (20, 40), (40, 60)\}$$

$$\mathcal{S} = \{(20, 35), (20, 55), (40, 55), (40, 75), (60, 95)\}$$

As matrizes booleanas que representam \mathcal{R} , \mathcal{S} e $\mathcal{S} \circ \mathcal{R}$ são

$$M = \left(\begin{array}{c|ccc} & 20 & 40 & 60 \\ \hline 10 & 1 & 0 & 1 \\ 20 & 0 & 1 & 0 \\ 30 & 0 & 0 & 0 \\ 40 & 0 & 0 & 1 \end{array} \right) N = \left(\begin{array}{c|cccc} & 35 & 55 & 75 & 95 \\ \hline 20 & 1 & 1 & 0 & 0 \\ 40 & 0 & 1 & 1 & 0 \\ 60 & 0 & 0 & 0 & 1 \end{array} \right) MN = \left(\begin{array}{c|cccc} & 35 & 55 & 75 & 95 \\ \hline 10 & 1 & 1 & 0 & 1 \\ 20 & 0 & 1 & 1 & 0 \\ 30 & 0 & 0 & 0 & 0 \\ 40 & 0 & 0 & 0 & 1 \end{array} \right)$$

6.4 Tipos de relações

Nesta seção daremos algumas propriedades de relações que são importantes em muitos contextos. Seja \mathcal{R} uma relação sobre um conjunto A . Dizemos que:

- \mathcal{R} é *reflexiva* sobre A se, e somente se, $(\forall a \in A) a\mathcal{R}a$. Isto significa que $(a, a) \in \mathcal{R}$ para todo $a \in A$.
- \mathcal{R} é *irreflexiva* sobre A se, e somente se, $(\forall a \in A) a\not\mathcal{R}a$. Isto significa que $(a, a) \notin \mathcal{R}$ para todo $a \in A$.
- \mathcal{R} é *simétrica* se, e somente se, $(\forall a, b \in A) a\mathcal{R}b \rightarrow b\mathcal{R}a$. Isto significa que se $(a, b) \in \mathcal{R}$ então $(b, a) \in \mathcal{R}$.
- \mathcal{R} é *anti-simétrica* se, e somente se, $(\forall a, b \in A) (a\mathcal{R}b) \wedge (b\mathcal{R}a) \rightarrow a = b$. Isto significa que se $(a, b) \in \mathcal{R}$ e $(b, a) \in \mathcal{R}$ então $a = b$.
- \mathcal{R} é *transitiva* se, e somente se, $(\forall a, b, c \in A) (a\mathcal{R}b) \wedge (b\mathcal{R}c) \rightarrow a\mathcal{R}c$. Isto significa que se $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$ então $(a, c) \in \mathcal{R}$.

Observe que os termos simétrica e anti-simétrica não são opostos: uma relação pode ser simétrica e anti-simétrica ao mesmo tempo, ou pode não ser nem simétrica nem anti-simétrica. Exemplos: Seja $A = \{1, 2, 3\}$ e $\mathcal{R}_1 = \{(1, 1), (2, 1), (1, 2), (3, 1)\}$. \mathcal{R}_1 não é simétrica pois $(3, 1) \in \mathcal{R}$ e $(1, 3) \notin \mathcal{R}$ nem anti-simétrica pois $(2, 1) \in \mathcal{R}$ e $(1, 2) \in \mathcal{R}$ e $1 \neq 2$. Se $\mathcal{R}_2 = \{(1, 1), (2, 2), (3, 3)\}$ então \mathcal{R}_2 é simétrica e anti-simétrica. Uma relação é anti-simétrica se não existem elementos distintos a e b tais que $a\mathcal{R}b$ e $b\mathcal{R}a$. Não é simétrica se contiver algum par (a, b) com $a \neq b$, e não conter o par (b, a) .

Observe também que uma relação pode ser nem reflexiva e nem irreflexiva, como mostra a relação \mathcal{R}_1 acima. Porém, se o conjunto A não é vazio, uma relação não pode ser ao mesmo tempo reflexiva e irreflexiva sobre A .

Finalmente, observe que uma relação pode satisfazer qualquer das propriedades acima por vacuidade, se não existirem elementos em A que satisfaçam as condições no lado esquerdo do conectivo ‘ \rightarrow ’. Por exemplo, a relação $\mathcal{R}_3 = \{(1, 2)\}$ é transitiva, porque não existem a, b e c tais que $(a\mathcal{R}_3b) \wedge (b\mathcal{R}_3c)$.

Exemplo 6.23: Considere o conjunto $A = \{1, 2, 3, 4\}$ e as seguintes relações sobre A :

- $\mathcal{R}_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 1), (4, 4)\}$.
- $\mathcal{R}_2 = \{(1, 1), (1, 2), (2, 1)\}$.
- $\mathcal{R}_3 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 1), (1, 4), (4, 4)\}$.
- $\mathcal{R}_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$.
- $\mathcal{R}_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$.
- $\mathcal{R}_6 = \{(3, 4)\}$.
- São reflexivas sobre A : $\mathcal{R}_1, \mathcal{R}_3$ e \mathcal{R}_5 .
- São irreflexivas sobre A : \mathcal{R}_4 e \mathcal{R}_6 .
- São simétricas: \mathcal{R}_2 e \mathcal{R}_3 .
- São anti-simétricas: $\mathcal{R}_4, \mathcal{R}_5$ e \mathcal{R}_6 .
- São transitivas: $\mathcal{R}_4, \mathcal{R}_5$ e \mathcal{R}_6 .

6.4.1 Composição e transitividade

O próximo teorema mostra como a operação de composição se relaciona com a propriedade transitiva de uma relação.

Teorema 6.3: Uma relação \mathcal{R} sobre um conjunto A é transitiva se, e somente se $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

Prova:

Seja \mathcal{R} uma relação. Vamos primeiro provar que, se \mathcal{R} é transitiva, então $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$. Seja $(a, b) \in \mathcal{R} \circ \mathcal{R}$. Pela definição de composição de relações, temos que $(\exists x \in A) (a, x) \in \mathcal{R} \wedge (x, b) \in \mathcal{R}$. Como \mathcal{R} é transitiva, concluímos que $(a, b) \in \mathcal{R}$. Logo $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$.

Vamos provar agora que, se $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, então \mathcal{R} é transitiva. Sejam a, b, c três elementos de A . Se $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$, então, pela definição de composição, temos que $(a, c) \in \mathcal{R} \circ \mathcal{R}$. Como $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, então $(a, c) \in \mathcal{R}$. Logo \mathcal{R} é transitiva.

Fim.

O teorema 6.3 pode ser reformulado: “Uma relação \mathcal{R} sobre um conjunto A é transitiva se e somente se $\mathcal{R}^2 \subseteq \mathcal{R}$.” Esse resultado pode ser generalizado:

Teorema 6.4: Uma relação \mathcal{R} é transitiva se e somente se $\mathcal{R}^n \subseteq \mathcal{R}$ para todo $n \geq 1$.

Prova:

Para provar a parte “somente se”, basta tomar $n = 2$ e usar o teorema 6.3. Para provar a segunda parte, vamos supor que \mathcal{R} é uma relação transitiva sobre um conjunto A , e provar que $\mathcal{R}^n \subseteq \mathcal{R}$, para todo $n \geq 1$, usando indução em n .

- *Base:* Para $n = 1$ a afirmação é verdadeira, pois $\mathcal{R}^1 = \mathcal{R} \subseteq \mathcal{R}$.
- *Hipótese de indução:* Vamos supor que $\mathcal{R}^k \subseteq \mathcal{R}$ para algum $k \geq 1$.
- *Passo:* Vamos demonstrar que $\mathcal{R}^{k+1} \subseteq \mathcal{R}$. Seja $(a, b) \in \mathcal{R}^{k+1}$; pela definição de potência, $(a, b) \in \mathcal{R}^k \circ \mathcal{R}$. Pela definição de composição, temos que $(\exists x \in A) (a, x) \in \mathcal{R}^k \wedge (x, b) \in \mathcal{R}$. Pela hipótese de indução, $\mathcal{R}^k \subseteq \mathcal{R}$, portanto $(x, b) \in \mathcal{R}$. Como \mathcal{R} é transitiva, temos que $(a, b) \in \mathcal{R}$.

Fim.

O que este teorema nos diz é que as potências de uma relação transitiva são sub-conjuntos da relação. Portanto se verificarmos que $\mathcal{R}^n \not\subseteq \mathcal{R}$, para algum $n \geq 1$, então podemos concluir que a relação não é transitiva.

Exercício 6.11: Prove esta afirmação, ou encontre um contra-exemplo: “Se $\mathcal{R}^4 \subseteq \mathcal{R}$, então \mathcal{R} é transitiva.”

6.4.2 Propriedades de relações usando matrizes

Se \mathcal{R} é uma relação sobre um conjunto finito A a matriz M é quadrada e as linhas e colunas tem os mesmos rótulos. Nesse caso, se usarmos a mesma ordem para linhas e colunas, várias propriedades da relação \mathcal{R} podem ser facilmente verificadas na matriz M :

1. Uma relação \mathcal{R} é reflexiva sobre A se, e somente se $(\forall i \in \{1, 2, \dots, n\}) a_i \mathcal{R} a_i$. Portanto \mathcal{R} é reflexiva sobre A e somente se $(\forall i \in \{1, 2, \dots, n\}) M_{i,i} = 1$; isto é, os elementos da diagonal de M são todos 1.
2. Uma relação \mathcal{R} é irreflexiva sobre A se, e somente se $(\forall i \in \{1, 2, \dots, n\}) a_i \not\mathcal{R} a_i$. Portanto \mathcal{R} é irreflexiva sobre A e somente se os elementos da diagonal de M são todos 0.
3. Uma relação \mathcal{R} é simétrica se, e somente se $(\forall i, j \in \{1, 2, \dots, n\}) a_i \mathcal{R} a_j \leftrightarrow a_j \mathcal{R} a_i$. Portanto \mathcal{R} é simétrica se, e somente se, a matriz M é simétrica, ou seja, ela é igual à sua transposta.
4. Uma relação \mathcal{R} é anti-simétrica se, e somente se $(\forall i, j \in \{1, 2, \dots, n\}) (a_i \mathcal{R} a_j \wedge a_j \mathcal{R} a_i) \rightarrow a_i = a_j$. Portanto \mathcal{R} é anti-simétrica se, e somente se não existem índices i e j com $i \neq j$ tais que $M_{i,j}$ e $M_{j,i}$ são simultaneamente iguais a 1.

Note que, no caso de uma relação anti-simétrica os elementos da diagonal são arbitrários. Note também que esta definição não corresponde ao conceito de “matriz anti-simétrica” da álgebra linear. Essa definição exige $M_{i,j} = -M_{j,i}$ o que implica que a diagonal é nula ($M_{i,i} = 0$).

Exemplo 6.24: Seja \mathcal{R} uma relação sobre um conjunto $A = \{a_1, a_2, a_3\}$ cuja matriz é

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Observe que:

- \mathcal{R} é reflexiva sobre A pois $m_{i,i} = 1$ para todo i .
- \mathcal{R} é simétrica pois M é simétrica.
- \mathcal{R} não é anti-simétrica pois $m_{1,2} = m_{2,1} = 1$.

Exercício 6.12: Se A é um conjunto com m elementos, quantas relações *reflexivas* distintas existem sobre A ? E quantas *irreflexivas*?

Exercício 6.13: Se A é um conjunto com m elementos, quantas relações *simétricas* distintas existem sobre A ? E quantas *anti-simétricas*?

6.5 Fechos de uma relação

6.5.1 Fecho reflexivo

Seja \mathcal{R} uma relação sobre um conjunto A . Se \mathcal{R} não é reflexiva sobre A , é porque não possui um ou mais pares da forma (a, a) com $a \in A$. Se acrescentarmos todos esses pares a \mathcal{R} , obtemos uma relação \mathcal{S} que é reflexiva sobre A e contém \mathcal{R} . Essa relação é chamada de *fecho reflexivo de \mathcal{R} sobre A* .

Exemplo 6.25: Sejam $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, a), (c, b)\}$. A relação $\mathcal{S} = \{(a, a), (a, b), (b, a), (c, b), (b, b), (c, c)\}$ é o fecho reflexivo de \mathcal{R} sobre A .

Exemplo 6.26: Seja a relação $\mathcal{R} = \{(a, b) : a, b \in \mathbb{Z} \wedge a < b\}$ sobre o conjunto dos números inteiros \mathbb{Z} . O fecho reflexivo \mathcal{S} é obtido incluindo na relação \mathcal{R} todos os pares $\{(a, a) : a \in \mathbb{Z}\}$. Ou seja, o fecho reflexivo de \mathcal{R} sobre \mathbb{Z} é

$$\mathcal{S} = \{(a, b) : a, b \in \mathbb{Z} \wedge a \leq b\}$$

Observe que o fecho reflexivo pode ser escrito como $\mathcal{R} \cup \mathcal{I}_A$. Observe também que qualquer outra relação \mathcal{T} que é reflexiva sobre A e contém \mathcal{R} deve conter \mathcal{I}_A , e portanto contém $\mathcal{I}_A \cup \mathcal{R} = \mathcal{S}$.

6.5.2 Fecho simétrico

De maneira análoga, se \mathcal{R} é uma relação qualquer, obtemos seu *fecho simétrico* acrescentando a \mathcal{R} todos os pares necessários para torná-la uma relação simétrica; isto é, todo par da forma (b, a) tal que $(a, b) \in \mathcal{R}$.

Exemplo 6.27: Sejam $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, b), (b, c), (c, a), (c, b)\}$. A relação $\mathcal{S} = \{(a, a), (a, b), (b, a), (b, b), (c, a), (b, c), (c, b)\}$ é o fecho simétrico de \mathcal{R} .

Exemplo 6.28: Seja a relação $\mathcal{R} = \{(a, b) : a, b \in \mathbb{Z} \wedge a < b\}$ sobre o conjunto dos números inteiros \mathbb{Z} . O fecho simétrico \mathcal{S} é obtido incluindo na relação \mathcal{R} todos os pares

$$\{(b, a) : a, b \in \mathbb{Z} \wedge a > b\}$$

. Ou seja, o fecho simétrico de \mathcal{R} é

$$\mathcal{S} = \{(a, b) : a, b \in \mathbb{Z} \wedge a \neq b\}$$

Observe que o fecho simétrico é simplesmente $\mathcal{R} \cup \mathcal{R}^{-1}$. Observe também que, como no caso do fecho reflexivo, qualquer outra relação simétrica \mathcal{T} que contém \mathcal{R} deve conter \mathcal{R}^{-1} , e portanto contém seu fecho simétrico $\mathcal{R} \cup \mathcal{R}^{-1}$.

6.5.3 Fecho transitivo

Vamos agora considerar o problema análogo de completar uma relação \mathcal{R} , se necessário, de modo a torná-la transitiva. Para isso, precisamos garantir que, para quaisquer pares (a, b) e (b, c) na relação, o par (a, c) também está na relação.

Podemos pensar que basta examinar todos os pares (a, c) e (b, c) que estão na relação dada \mathcal{R} . Entretanto, isso não é suficiente. Por exemplo, considere a relação

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

Esta relação falha a definição de relação transitiva em exatamente dois casos:

$$\begin{aligned} (1, 2) \in \mathcal{R} \wedge (2, 3) \in \mathcal{R} \quad \text{mas} \quad (1, 3) \notin \mathcal{R} \\ (2, 3) \in \mathcal{R} \wedge (3, 4) \in \mathcal{R} \quad \text{mas} \quad (2, 4) \notin \mathcal{R} \end{aligned}$$

Se acrescentarmos os pares $(1, 3)$ e $(2, 4)$, obtemos a relação

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

Mas esta relação ainda não é transitiva; pois ela possui $(1, 3)$ e $(3, 4)$ mas não possui $(1, 4)$. Observe que esta falha de transitividade foi revelada quando acrescentamos o par $(1, 3)$ à relação.

Se acrescentarmos o par que falta, $(1, 4)$, obtemos

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

que é transitiva.

Os pares que faltam em \mathcal{R} são da forma (a, c) tais que existe algum b com $(a, b) \in \mathcal{R}$ e $(b, c) \in \mathcal{R}$. Ou seja, são os pares de $\mathcal{R} \circ \mathcal{R} = \mathcal{R}^2$. Portanto, ao acrescentarmos esses pares estamos construindo

a relação $\mathcal{R}' = \mathcal{R} \cup \mathcal{R}^2$. Pela mesma razão, os pares que ainda faltam em \mathcal{R}' estão na relação $\mathcal{R}' \circ \mathcal{R}' = (\mathcal{R} \cup \mathcal{R}^2)^2$, que (pelo exercício 6.8) é a relação $\mathcal{R}^2 \cup \mathcal{R}^3 \cup \mathcal{R}^4$. Portanto, acrescentando esses pares obtemos $\mathcal{R}'' = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \mathcal{R}^4$. No próximo passo, obtemos $\mathcal{R} \cup \mathcal{R}^2 \cup \dots \cup \mathcal{R}^7 \cup \mathcal{R}^8$. E assim por diante.

Por estas considerações, o *fecho transitivo* de \mathcal{R} , denotado por \mathcal{R}^* é definido como sendo a união de todas as potências de \mathcal{R} , isto é

$$\mathcal{R}^* = \mathcal{R} \cup \mathcal{R}^2 \cup \mathcal{R}^3 \cup \dots \quad (6.1)$$

que pode ser escrita mais sucintamente como

$$\mathcal{R}^* = \bigcup_{k=1}^{\infty} \mathcal{R}^k \quad (6.2)$$

(Veja seção 8.8.) Ou seja, um par (a, b) está em \mathcal{R}^* se, e somente se, existe um inteiro $k \geq 1$ tal que $(a, b) \in \mathcal{R}^k$.

Se \mathcal{R} é uma relação sobre um conjunto *finito* A , a união eventualmente deixa de crescer após um número finito de termos; pois os pares que podem ser acrescentados pertencem ao conjunto $A \times A$, que é finito. Pode-se mostrar que, se A tem n elementos, o processo termina com o termo \mathcal{R}^n , no máximo. Nesse caso, a relação \mathcal{R}^* assim obtida é uma relação transitiva, por construção.

No caso de A ser finito, também podemos escrever a fórmula (6.3) em termos das matrizes booleanas. Se M é a matriz de \mathcal{R} , a matriz M^* de \mathcal{R}^* é dada pela fórmula

$$M^* = \bigvee_{k=1}^n M^k = M \vee M^2 \vee M^3 \vee \dots \vee M^n \quad (6.3)$$

Caso o conjunto A seja infinito, o processo pode nunca terminar: após cada acréscimo de pares que faltam podem surgir novos casos de falha de transitividade. Nesse caso, a união (6.3) precisa incluir todas as potências de \mathcal{R} . Precisamos então provar o seguinte resultado:

Teorema 6.5: Para qualquer relação \mathcal{R} , a relação \mathcal{R}^* é transitiva.

Prova:

Sejam a, b, c elementos tais que (a, b) e (b, c) estão em \mathcal{R}^* . Precisamos provar que (a, c) também está em \mathcal{R}^* .

Pela definição de \mathcal{R}^* , existem inteiros $i \geq 1$ e $j \geq 1$ tais que $(a, b) \in \mathcal{R}^i$ e $(b, c) \in \mathcal{R}^j$. Portanto (a, c) está na composição $\mathcal{R}^j \circ \mathcal{R}^i$, que, pelo exercício 6.10, é igual a \mathcal{R}^{i+j} . Portanto o par (a, c) também está em \mathcal{R}^* .

Fim.

Por outro lado, o teorema a seguir mostra que o fecho transitivo \mathcal{R}^* calculado pela fórmula (6.3) não tem nenhum par supérfluo:

Teorema 6.6: Para qualquer relação \mathcal{R} , qualquer relação transitiva que contém \mathcal{R} contém o fecho transitivo \mathcal{R}^* de \mathcal{R} .

Prova:

Seja \mathcal{R} uma relação qualquer, e seja \mathcal{S} uma relação que contém \mathcal{R} . Pelo teorema 6.2, para todo $n \geq 1$, temos que $\mathcal{R}^n \subseteq \mathcal{S}^n$. Pelo teorema 6.4, temos que $\mathcal{S}^n = \mathcal{S}$; logo $\mathcal{R}^n \subseteq \mathcal{S}$. Uma vez que todos os termos da fórmula (6.3) estão contidos em \mathcal{S} , então a união de todos esses termos \mathcal{R}^* também está.

Fim.

Os dois teoremas acima implicam que o fecho transitivo \mathcal{R}^* definido pela fórmula (6.3) é a *única* relação transitiva que contém \mathcal{R} e está contida em qualquer relação transitiva que contém \mathcal{R} . Portanto ela é também a menor relação transitiva que contém \mathcal{R} .

6.5.4 Fecho em geral

De maneira geral, sejam \mathcal{R} uma relação em um conjunto A , \mathbf{P} uma propriedade de relações, e \mathcal{S} uma relação em A com a propriedade \mathbf{P} . Dizemos que \mathcal{S} é o *fecho* da relação \mathcal{R} com respeito à *propriedade* \mathbf{P} , se \mathcal{S} contém \mathcal{R} e está contida em toda relação que possui a propriedade \mathbf{P} e contém \mathcal{R} .

Em outras palavras, \mathcal{S} é o fecho de \mathcal{R} com respeito à propriedade \mathbf{P} se

- $\mathcal{R} \subseteq \mathcal{S}$.
- \mathcal{S} satisfaz a propriedade \mathbf{P} .
- Para toda relação \mathcal{T} em A , se $\mathcal{R} \subseteq \mathcal{T}$ e \mathcal{T} satisfaz a propriedade \mathbf{P} , então $\mathcal{S} \subseteq \mathcal{T}$.

A relação \mathcal{R} pode ter ou não ter a propriedade \mathbf{P} . Se \mathcal{R} tiver a propriedade \mathbf{P} então $\mathcal{R} = \mathcal{S}$.

O fecho de uma relação com respeito a uma determinada propriedade pode ou não existir. Veja o exemplo a seguir:

Exemplo 6.29: Sejam $A = \{1, 2, 3\}$, $\mathcal{R} = \{(1, 1), (1, 2), (2, 2), (3, 3)\}$ e $\mathbf{P}(\mathcal{R}) = \text{“}\mathcal{R} \text{ não é reflexiva sobre } A\text{”}$. Observe que qualquer relação contendo \mathcal{R} conterá $\{(1, 1), (2, 2), (3, 3)\}$, portanto não existe nenhuma relação, que não seja reflexiva sobre A , e contenha \mathcal{R} .

Neste exemplo, o fecho não existe porque é impossível completar \mathcal{R} de modo a satisfazer \mathbf{P} . No exemplo abaixo, o fecho não existe porque há duas ou mais maneiras de fazer isso, mas elas são incompatíveis:

Exemplo 6.30: Sejam $A = \{1, 2\}$, $\mathcal{R} = \{(1, 1), (2, 2)\}$ e $\mathbf{P}(\mathcal{R}) = \text{“}\mathcal{R} \text{ tem 3 pares”}$. As duas relações $\mathcal{S}_1 = \{(1, 1), (1, 2), (2, 2)\}$ e $\mathcal{S}_2 = \{(1, 1), (2, 1), (2, 2)\}$ são relações que satisfazem a propriedade \mathbf{P} e contém \mathcal{R} ; porém, a única relação \mathcal{S} que está contida em \mathcal{S}_1 e em \mathcal{S}_2 e contém \mathcal{R} é a própria relação \mathcal{R} , que não satisfaz \mathbf{P} .

Exercício 6.14: Encontre os fechos reflexivo, simétrico e transitivo das seguintes relações:

- $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, c), (c, b)\}$.
- $A = \{0, 1, 2, 3\}$ e $\mathcal{R} = \{(0, 1), (1, 1), (1, 2), (2, 0), (2, 2), (3, 0)\}$.

Exercício 6.15: Sejam $A = \{1, 2, 3, 4, 5\}$ e $\mathcal{R} = \{(1, 3), (2, 4), (3, 1), (3, 5), (4, 3), (5, 1), (5, 2), (5, 4)\}$. Encontre as potências $\mathcal{R}^2, \mathcal{R}^3, \mathcal{R}^4, \mathcal{R}^5, \mathcal{R}^6$ e o fecho transitivo \mathcal{R}^* .

Exercício 6.16: Encontre a menor relação contendo $A = \{(1, 2), (1, 4), (3, 3), (4, 1)\}$ que é:

- Simétrica e reflexiva sobre A .
- Reflexiva sobre A e transitiva.
- Simétrica e transitiva.
- Reflexiva sobre A , simétrica e transitiva.

Exercício 6.17: Sejam \mathcal{R}_1 e \mathcal{R}_2 relações sobre o conjunto A , tais que $\mathcal{R}_1 \subseteq \mathcal{R}_2$.

- Sejam \mathcal{S}_1 e \mathcal{S}_2 os fechos reflexivos de \mathcal{R}_1 e \mathcal{R}_2 , respectivamente. Prove que $\mathcal{S}_1 \subseteq \mathcal{S}_2$.
- Enuncie os teoremas análogos para os fechos simétricos e transitivos. Prove esses teoremas, ou encontre contra-exemplos.

Exercício 6.18: Sejam \mathcal{R}_1 e \mathcal{R}_2 relações sobre o conjunto A , e $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$.

- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos reflexivos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$.
- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos simétricos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S}_1 \cup \mathcal{S}_2 = \mathcal{S}$.
- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos transitivos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S}_1 \cup \mathcal{S}_2 \subseteq \mathcal{S}$, e encontre um exemplo em que a inclusão é própria.

Exercício 6.19: Sejam \mathcal{R}_1 e \mathcal{R}_2 relações sobre o conjunto A , e $\mathcal{R} = \mathcal{R}_1 \cap \mathcal{R}_2$.

- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos reflexivos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S} = \mathcal{S}_1 \cap \mathcal{S}_2$.
- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos simétricos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S} \subseteq \mathcal{S}_1 \cap \mathcal{S}_2$, e mostre com um exemplo que a inclusão pode ser própria.
- Sejam $\mathcal{S}_1, \mathcal{S}_2$ e \mathcal{S} os fechos transitivos de $\mathcal{R}_1, \mathcal{R}_2$ e \mathcal{R} , respectivamente. Prove que $\mathcal{S} \subseteq \mathcal{S}_1 \cap \mathcal{S}_2$, e mostre com um exemplo que a inclusão pode ser própria.

Exercício 6.20: Seja \mathcal{R} a relação sobre o conjunto dos números inteiros positivos tal que $a\mathcal{R}b$ se e somente se existe um número primo p tal que $a = pb$. Qual é o fecho reflexivo \mathcal{S} de \mathcal{R} ? Encontre o fecho transitivo \mathcal{T} de \mathcal{R} .

6.6 Relações de ordem

Definição 6.2: Uma relação \mathcal{R} sobre um conjunto A é uma *relação de ordem* se ela é reflexiva sobre A , anti-simétrica e transitiva.

Exemplo 6.31: Sejam $A = \mathbb{R}$ e $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}, : x \leq y\}$.

- \mathcal{R} é reflexiva sobre A pois $(\forall x \in \mathbb{R}) x \leq x$ logo $(\forall x \in \mathbb{R}) x\mathcal{R}x$.
- \mathcal{R} é transitiva pois $(\forall x, y, z \in \mathbb{R}) ((x \leq y \wedge y \leq z) \rightarrow x \leq z)$. Portanto

$$(\forall x, y, z \in \mathbb{R}) (x\mathcal{R}y \wedge y\mathcal{R}z) \rightarrow x\mathcal{R}z$$

- \mathcal{R} é anti-simétrica pois $(\forall x, y \in \mathbb{R}) (x \leq y \wedge y \leq x) \rightarrow x = y$. Portanto

$$(\forall x, y \in \mathbb{R}) (x\mathcal{R}y \wedge y\mathcal{R}x) \rightarrow x = y$$

Exemplo 6.32: Sejam $\mathbb{P}(A)$ o conjunto potência de um conjunto A e

$$S = \{ (X, Y) \in \mathbb{P}(A) : X \subseteq Y \}$$

- \mathcal{R} é reflexiva sobre $\mathbb{P}(A)$ pois $(\forall X \in \mathbb{P}(A)) X \subseteq X$ logo $(\forall X \in \mathbb{P}(A)) X\mathcal{R}X$.
- \mathcal{R} é transitiva pois $(\forall X, Y, Z \in \mathbb{P}(A)) (X \subseteq Y \wedge Y \subseteq Z) \rightarrow X \subseteq Z$. Portanto $(\forall X, Y, Z \in \mathbb{P}(A)) (X\mathcal{R}Y \wedge Y\mathcal{R}Z) \rightarrow X\mathcal{R}Z$.
- \mathcal{R} é anti-simétrica pois $(\forall X, Y \in \mathbb{P}(A)) (X \subseteq Y \wedge Y \subseteq X) \rightarrow X = Y$. Portanto $(\forall X, Y \in \mathbb{P}(A)) (X\mathcal{R}Y \wedge Y\mathcal{R}X) \rightarrow X = Y$.

Observe que se \mathcal{R} é uma relação de ordem sobre um conjunto A , e $A' \subseteq A$, a restrição de \mathcal{R} a A' é uma relação de ordem sobre A' .

Se \mathcal{R} é uma relação de ordem sobre um conjunto A , o par (A, \mathcal{R}) é chamado um *conjunto ordenado*. Por exemplo, (\mathbb{N}, \leq) é um conjunto ordenado (entendendo-se que ' \leq ' aqui é a restrição da relação "menor ou igual" aos números naturais). Outro exemplo de conjunto ordenado é $(\mathbb{P}(A), \subseteq)$, para qualquer conjunto A .

Exercício 6.21: Seja \mathcal{R} a relação sobre o conjunto dos números inteiros positivos tal que $a\mathcal{R}b$ se e somente se existe um inteiro positivo k tal que $a = kb$. Mostre que \mathcal{R} é uma relação de ordem.

Exercício 6.22: Seja A o conjunto dos inteiros de 0 a 9, e \mathcal{R} a relação sobre A tal que $a\mathcal{R}b$ se e somente se a é par e b é ímpar, ou ambos são pares e $a \leq b$, ou ambos são ímpares e $a \geq b$. Esta é uma relação de ordem?

Exercício 6.23: Considere a relação \mathcal{R} sobre os pares ordenados de inteiros $\mathbb{Z} \times \mathbb{Z}$ tal que

$$(a, b)\mathcal{R}(c, d) \leftrightarrow (a \leq c) \vee (b \leq d)$$

para quaisquer inteiros a, b, c e d . Esta é uma relação de ordem?

Exercício 6.24: Para quaisquer relações de ordem \mathcal{R} e \mathcal{S} sobre um conjunto A , a relação $\mathcal{R} \cup \mathcal{S}$ é sempre uma relação de ordem sobre A ? E a relação $\mathcal{R} \cap \mathcal{S}$? Prove suas respostas.

Exercício 6.25: Seja S o conjunto de todos os arquivos em um sistema de arquivos, e \mathcal{R} a relação sobre S tal que $a\mathcal{R}b$ se e somente se o arquivo a contém uma cópia do conteúdo do arquivo b , possivelmente com informações adicionais antes do início de b ou depois do fim. A relação \mathcal{R} é uma relação de ordem?

6.6.1 Diagrama de Hasse

Podemos representar graficamente um conjunto ordenado (A, \mathcal{R}) , onde A é finito e não muito grande, por um diagrama de pontos e linhas, chamado *diagrama de Hasse* (em homenagem ao matemático alemão Helmut Hasse, 1898–1979).

Neste diagrama, cada elemento de A é representado por um ponto do plano, com posição arbitrária, exceto pela regra de que, para todo par $(a, b) \in \mathcal{R}$ com $a, b \in A$ e $a \neq b$, o ponto que representa a deve estar abaixo do ponto que representa b . Cada um desses pares é representado por uma linha reta ligando a com b , exceto que pares que podem ser deduzidos por transitividade não são desenhados.

Para ilustrar a construção deste diagrama, vamos usar o conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, e a seguinte relação sobre A :

$$\begin{aligned} \mathcal{R} = \{ & (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 7), \\ & (2, 2), (2, 3), (2, 4), (2, 5), \\ & (3, 3), (3, 4), (3, 5), \\ & (4, 4), (4, 5), \\ & (5, 5), \\ & (6, 6), (6, 9), (6, 5), \\ & (7, 7), (7, 4), (7, 5), \\ & (8, 8), (8, 7), (8, 4), (8, 5), \\ & (9, 9), (9, 5) \end{aligned}$$

Podemos representar o conjunto A e os pares de \mathcal{R} pelo diagrama de pontos e setas da figura 6.3 (à esquerda). Observe que, da maneira como os pontos foram dispostos, todas as setas apontam de baixo para cima; portanto não é necessário indicar sua direção. Sabendo que \mathcal{R} é uma relação de ordem, podemos também omitir todos os laços, e todas as linhas que podem ser deduzidas pela transitividade; como $(1, 3)$, por exemplo, que pode ser deduzida pelos pares $(1, 2)$ e $(2, 3)$. O resultado dessas simplificações é o diagrama de Hasse (à direita).

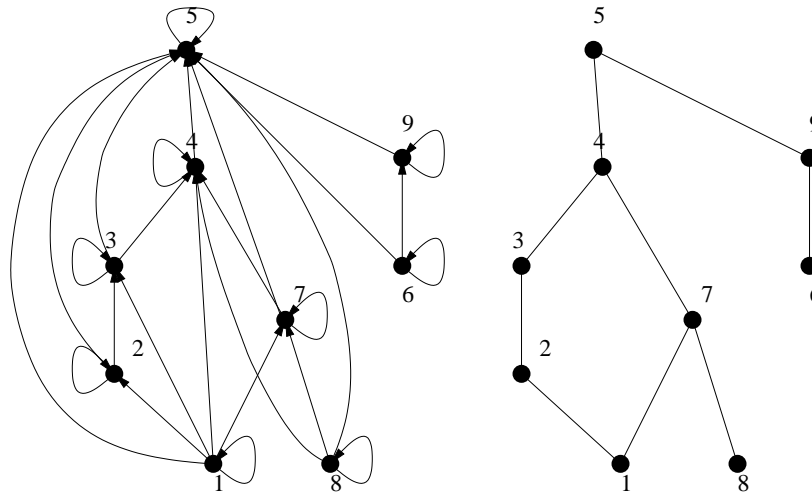


Figura 6.3: Diagrama de pontos e setas do conjunto ordenado (A, \mathcal{R}) (à esquerda) e o diagrama de Hasse (à direita).

Observe que o diagrama de Hasse contém toda a informação necessária para determinar exatamente a relação de ordem \mathcal{R} .

6.6.2 Relações de ordem estrita

Definição 6.3: Uma relação \mathcal{R} sobre um conjunto A é uma *relação de ordem estrita* se ela é irreflexiva sobre A , anti-simétrica e transitiva.

Exemplo 6.33: Sejam $A = \mathbb{R}$ e $\mathcal{R} = \{(x, y) \in \mathbb{R} \times \mathbb{R}, : x < y\}$.

- \mathcal{R} é irreflexiva sobre A pois $(\forall x \in \mathbb{R}) \neg(x < x)$ logo $(\forall x \in \mathbb{R}) x \not\mathcal{R}x$.
- \mathcal{R} é transitiva pois $(\forall x, y, z \in \mathbb{R}) ((x < y \wedge y < z) \rightarrow x < z)$. Portanto

$$(\forall x, y, z \in \mathbb{R}) (x\mathcal{R}y \wedge y\mathcal{R}z) \rightarrow x\mathcal{R}z$$

- \mathcal{R} é anti-simétrica, pois $(\forall x, y \in \mathbb{R}) \neg((x < y \wedge y < x))$. Portanto, por vacuidade,

$$(\forall x, y \in \mathbb{R}) (x\mathcal{R}y \wedge y\mathcal{R}x) \rightarrow x = y$$

Note que uma relação de ordem estrita não é um tipo particular de relação de ordem. Porém, toda relação de ordem estrita \mathcal{R} pode ser obtida de uma relação de ordem \mathcal{S} excluindo-se todos os pares da forma (a, a) . Reciprocamente, toda relação de ordem \mathcal{S} sobre um conjunto A é a união $\mathcal{R} \cup \mathcal{I}_A$ onde \mathcal{R} é uma relação de ordem estrita sobre A . Note que, para quaisquer $a, b \in A$

$$a\mathcal{R}b \leftrightarrow (a\mathcal{S}b \wedge a \neq b)$$

$$a\mathcal{S}b \leftrightarrow (a\mathcal{R}b \vee a = b)$$

Dizemos que \mathcal{R} é a *ordem estrita associada à ordem \mathcal{S}* , e vice-versa.

O diagrama de Hasse pode ser construído também a partir de uma ordem estrita, e é igual ao diagrama da relação de ordem associada.

Exercício 6.26: Seja A um conjunto de caixas, e \mathcal{R} a relação sobre A tal que $a\mathcal{R}b$ se e somente se a caixa a cabe dentro da caixa b . Prove que esta é uma relação de ordem estrita.

6.6.3 Ordem total

Dizemos que dois elementos a, b são *comparáveis por* uma relação \mathcal{R} se $a\mathcal{R}b$ ou $b\mathcal{R}a$.

Definição 6.4: Uma relação \mathcal{R} é uma *ordem total* sobre um conjunto A (ou *ordem linear*) se, e somente se \mathcal{R} é uma relação de ordem sobre A e quaisquer dois elementos de A são comparáveis por \mathcal{R} .

Portanto uma relação de ordem \mathcal{R} é total se, quaisquer que sejam a e b em A , $(a, b) \in \mathcal{R}$ ou $(b, a) \in \mathcal{R}$.

Observe que a relação \leq (exemplo 6.33) é uma ordem total sobre \mathbb{R} , pois $(\forall a, b \in \mathbb{R}) a \leq b \vee b \leq a$. Por outro lado, a relação \subseteq (exemplo 6.32) não é uma ordem total quando A tem pelo menos dois elementos, pois nesse caso existem sub-conjuntos distintos X e Y em $\mathbb{P}(A)$ tais que nem $X \subseteq Y$ nem $Y \subseteq X$. Por exemplo, se $A = \{1, 2\}$, podemos tomar $X = \{1\}$ e $Y = \{2\}$.

Analogamente, dizemos que uma ordem estrita \mathcal{R} sobre um conjunto A é *total* se e somente se quaisquer dois elementos *distintos* de A são comparáveis por \mathcal{R} .

Exercício 6.27: A ordem estrita sobre um conjunto de caixas definida no exercício 6.26 é uma ordem total?

Exercício 6.28: Descreva o diagrama de Hasse de uma ordem total sobre um conjunto finito A .

Se \mathcal{R} é uma relação de ordem total sobre A , o par (A, \mathcal{R}) é chamado de *conjunto totalmente ordenado*.

Exercício 6.29: Seja \mathcal{R} uma relação sobre um conjunto A , e seja \mathcal{S} a relação $(A \times A) \setminus \mathcal{R}$. Mostre que \mathcal{R} é uma relação de ordem total sobre A se e somente se \mathcal{S} é uma relação de ordem estrita total sobre A .

6.6.4 Ordem lexicográfica

Uma ordem muito importante no dia a dia, e em computação, é a *ordem alfabética* definida sobre palavras, nomes, etc.. Por exemplo, nesta ordem “hoje” vem antes de “ontem”, “biscoito” vem antes de “bolacha”, “porco” vem antes de “porta”, e “sol” vem antes de “soldado”.

Observe que esta ordem é baseada na ordem tradicional das letras do alfabeto: a, b, c, ..., z. A regra é: para decidir se uma palavra vem antes da outra, compara-se a primeira letra de uma com a primeira letra da outra. Se forem diferentes, a ordem das palavras é a mesma das letras. Se as palavras começam com a mesma letra, compara-se a segunda letra de uma com a segunda da outra. Se persistir o empate, consideram-se as terceiras letras, as quartas letras, e assim por diante — até haver um desempate (letras diferentes na mesma posição das duas palavras), ou uma das palavras terminar. Neste último caso (como no exemplo de “sol” e “soldado”), convencionam-se que a palavra que termina primeiro vem antes da outra.

Uma idéia semelhante pode ser utilizada para ordenar pares de reais. Seja a relação \leq_2 definida sobre os pares $\mathbb{R} \times \mathbb{R}$, pela fórmula

$$(a_1, a_2) \leq_2 (b_1, b_2) \leftrightarrow (a_1 < b_1) \vee (a_1 = b_1 \wedge a_2 \leq b_2)$$

Note a semelhança entre a relação \leq_2 e a ordem alfabética de palavras.

Este conceito pode ser generalizado para sequências de “letras” arbitrárias e ordenações arbitrárias dessas “letras”. Seja \mathcal{R} uma relação de ordem sobre um conjunto A . Vamos denotar por A^* o conjunto de todas as sequências de elementos de A , e $()$ a sequência vazia. Considere a relação \mathcal{R}^* definida recursivamente sobre A^* , da seguinte maneira:

1. $() \mathcal{R}^* b$ para qualquer sequência $b \in A^*$.
2. $b \mathcal{R}^* ()$ para qualquer sequência não vazia a em A^* .
3. Se a e b são sequências não vazias em A^* , sejam a_1 e b_1 os elementos iniciais de a e b , e a' , b' o que resta de a e b retirando-se estes elementos iniciais. Então temos que $a \mathcal{R}^* b$ se, e somente se,

$$(a_1 \neq b_1 \wedge a_1 \mathcal{R} b_1) \vee (a_1 = b_1 \wedge a' \mathcal{R}^* b')$$

Observe que esta definição recursiva permite determinar, em um número finito de passos, se qualquer par (a, b) de seqüências de A^* está na relação \mathcal{R}^* ou não. Prova-se (veja exercícios 6.30, 6.31 e 6.32) que a relação \mathcal{R}^* definida desta forma é uma relação de ordem. Prova-se também que \mathcal{R}^* é uma ordem total se e somente se \mathcal{R} é total (veja exercício 6.33).

A relação \mathcal{R}^* acima é chamada de *ordem lexicográfica induzida por \mathcal{R}* .

Exercício 6.30: Prove que a relação \mathcal{R}^* definida acima é reflexiva. (Dica: use indução no número n de elementos da mais curta entre as duas seqüências.)

Exercício 6.31: Prove que a relação \mathcal{R}^* definida acima é anti-simétrica.

Exercício 6.32: Prove que a relação \mathcal{R}^* definida acima é transitiva.

Exercício 6.33: Prove que a relação de ordem \mathcal{R}^* definida acima é total se e somente se \mathcal{R} é total.

6.6.5 Ordens “parciais”

Fora de contextos matemáticos, a palavra “parcial” geralmente significa “incompleto”, e portanto o oposto de “total”. Em matemática, entretanto, muitos autores usam “relação de ordem parcial” como sinônimo de “relação de ordem”. Para esses autores, as ordens totais são casos particulares de ordens parciais.

Esses autores também se referem a um conjunto ordenado (A, \mathcal{R}) como “conjunto parcialmente ordenado”, (em inglês, *partially ordered set* ou *poset*) — mesmo que a relação \mathcal{R} seja uma ordem total.

Para outros autores, entretanto, “ordem parcial” pode significar uma ordem que não é total. O leitor deve ficar atento para esses dois sentidos da palavra “parcial”. Para evitar ambiguidades, pode-se evitar essa palavra, usando “relação de ordem” para o caso geral, e “ordem total” ou “ordem não total” para os dois tipos.

6.6.6 Elementos mínimos e máximos

Seja \mathcal{R} uma relação de ordem sobre um conjunto X , e A um subconjunto de X . Um *elemento mínimo de A sob \mathcal{R}* é um elemento $m \in A$ tal que $(m, a) \in \mathcal{R}$ para todo $a \in A$.

Exemplo 6.34: Seja $A = \{2, 4, 6, 8\} \subseteq \mathbb{Z}$, e seja \mathcal{R} a relação ‘ \leq ’ (“menor ou igual”) sobre \mathbb{Z} . O inteiro 2 é um mínimo de A sob \mathcal{R} , pois $(2, a) \in \mathcal{R}$ (ou seja $2 \leq a$) para todo $a \in A$.

Exemplo 6.35: Considere o conjunto de conjuntos

$$A = \{ \{1, 2, 4\}, \{2, 4\}, \{2, 3, 4\}, \{2, 4, 5\}, \{2, 3, 4, 6\} \}$$

e seja \mathcal{R} a relação “ \subseteq ” entre conjuntos. O elemento $\{2, 4\}$ de A é mínimo sob \mathcal{R} , pois $\{2, 4\} \subseteq b$ para todo conjunto $b \in A$.

O conceito de *elemento máximo de A sob \mathcal{R}* é inteiramente simétrico. Ou seja, um elemento m de A é máximo sob uma relação \mathcal{R} tal que $(a, m) \in \mathcal{R}$ para todo $a \in A$.

No diagrama de Hasse de \mathcal{R} , o elemento mínimo existe se há um único ponto no diagrama a partir do qual é possível alcançar qualquer outro ponto por uma seqüência de linhas, todas elas

percorridas no sentido de baixo para cima. O elemento máximo, se existe, pode ser identificado de maneira análoga, isto é, se a partir dele podemos alcançar qualquer outro ponto percorrendo uma sequência de linhas no sentido descendente.

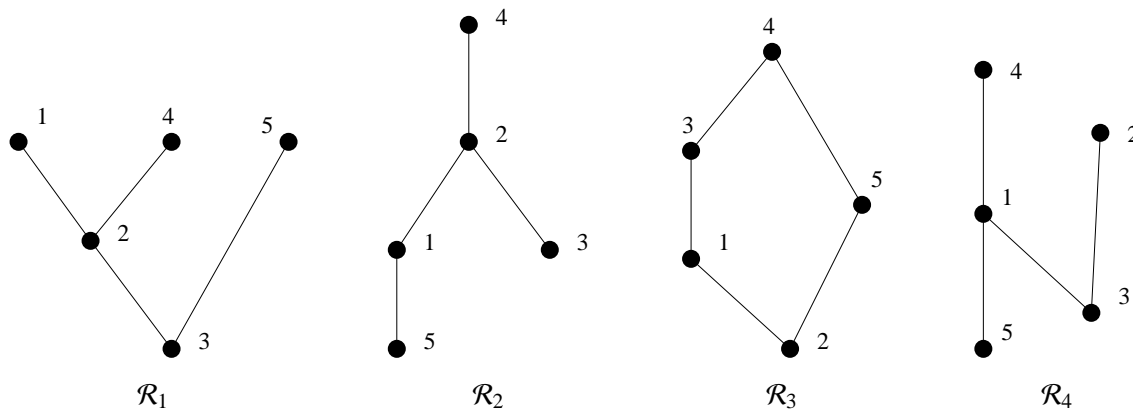


Figura 6.4: Diagramas de Hasse de quatro relações de ordem sobre o conjunto $\{1, 2, 3, 4, 5\}$. Na relação \mathcal{R}_1 , o elemento 3 é mínimo e não existe elemento máximo. Na relação \mathcal{R}_2 , o elemento 4 é máximo, e não há elemento mínimo. Na relação \mathcal{R}_3 , o elemento 2 é mínimo e 4 é máximo. Na relação \mathcal{R}_4 não existe nem mínimo nem máximo.

Se \mathcal{R} é uma relação de ordem total, e o conjunto A é finito, sempre existe um elemento mínimo. Se \mathcal{R} não é uma ordem total, ou se A é infinito, o mínimo pode existir ou não. Em qualquer caso, se existe um elemento mínimo, ele é único. As mesmas observações são válidas para o máximo.

Exemplo 6.36: Seja A o conjunto dos inteiros pares, e \mathcal{R} a relação “ \leq ” (menor ou igual) sobre \mathbb{Z} . Não existe nenhum elemento mínimo de A sob \mathcal{R} , pois para qualquer inteiro $m \in A$ o par $(m-2, m)$, por exemplo, está em \mathcal{R} .

É importante observar que o fato de um elemento ser mínimo depende tanto do conjunto A quanto da relação \mathcal{R} . Um elemento que é mínimo sob \mathcal{R} pode não ser mínimo sob outra relação \mathcal{S} . Em particular, um elemento mínimo sob \mathcal{R} é um elemento máximo sob \mathcal{R}^{-1} , e vice-versa.

Este fato pode gerar confusões se existe uma ordem “usual” para os elementos de A , distinta da ordem \mathcal{R} . Por exemplo, no conjunto A acima, o elemento 8 é mínimo, e 2 é máximo, sob a ordem “ \geq ”.

Exercício 6.34: Seja A o conjunto das palavras de 3 letras da língua portuguesa, e \mathcal{R} a relação tal que $a\mathcal{R}b$ se e somente se a palavra a vem antes da palavra b no dicionário. Quais são os elementos mínimo e máximo de A sob \mathcal{R} ?

Exercício 6.35: Seja A o conjunto das seqüências de 4 bits (algarismos 0 ou 1), e \mathcal{R} a relação tal que $a\mathcal{R}b$ se e somente se cada bit de a é menor ou igual ao bit correspondente de b . Assim, por exemplo, $0100\mathcal{R}1100$, mas $1001\not\mathcal{R}0101$. Quais são os elementos mínimo e máximo de A sob \mathcal{R} ?

6.6.7 Elementos minimais e maximais

Seja \mathcal{R} uma relação de ordem sobre um conjunto X , e A um subconjunto de X . Um *elemento minimal de A sob \mathcal{R}* é um elemento $m \in A$ tal que não existe nenhum $a \in A$, diferente de m , com $(a, m) \in \mathcal{R}$.

Exemplo 6.37: Seja $A = \{1, 2, 3, 4, 5, 6\}$ e $\mathcal{R} = \{(1, 3), (2, 3), (1, 4), (2, 4), (3, 4), (5, 6)\}$. O inteiro 2, por exemplo, é um elemento minimal de A sob \mathcal{R} , pois não existe nenhum par $(a, 2)$ na relação. Os elementos minimais de A sob \mathcal{R} são 1, 2, e 5.

Exemplo 6.38: Seja $A = \mathbb{N} \setminus \{0, 1\}$ e \mathcal{R} a relação “é divisor próprio de”; isto é, $\mathcal{R} = \{(x, y) : x \in A \wedge y \in A \wedge x < y \wedge (\exists k \in \mathbb{N} \setminus \{0, 1\}) (y = kx)\}$. O número 21 não é minimal sob \mathcal{R} pois existem pares $(a, 21)$ em \mathcal{R} , por exemplo $(3, 21)$. O número 17 é minimal sob \mathcal{R} pois não existe nenhum par $(a, 17)$ em \mathcal{R} . Note que os elementos minimais de A sob \mathcal{R} são os números primos.

Como estes exemplos mostram, uma relação pode não ter elementos minimais, ou pode ter mais de um elemento minimal. É fácil mostrar que um elemento mínimo de A sob \mathcal{R} , se existir, é também um elemento minimal (e o único elemento minimal em A). O contrário não é verdadeiro: um elemento minimal pode não ser mínimo.

Da mesma forma definimos um *elemento maximal de A sob \mathcal{R}* como um elemento m de A tal que não existe nenhum a em A , diferente de m , tal que $(m, a) \in \mathcal{R}$.

No diagrama de Hasse de \mathcal{R} , um elemento minimal é qualquer ponto do qual não sai nenhuma linha descendente. Um elemento maximal é um elemento do qual não sai nenhuma linha ascendente. Veja a figura 6.5

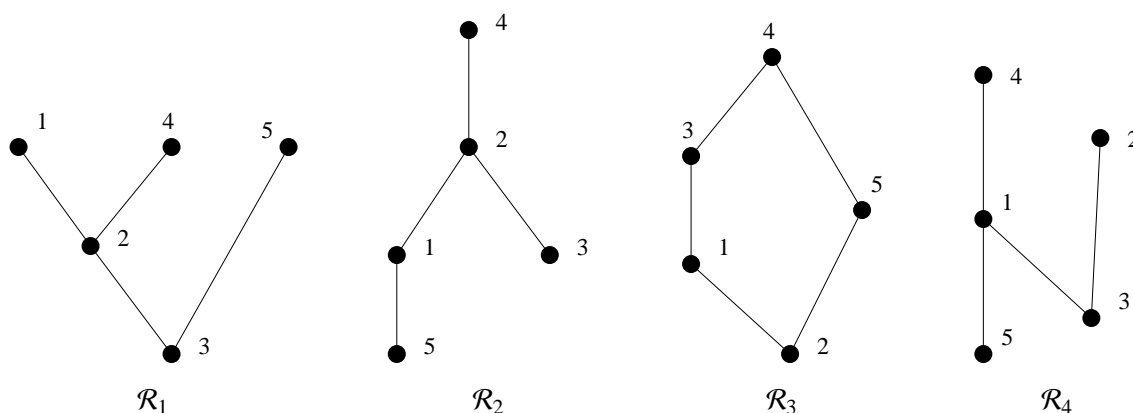


Figura 6.5: Diagramas de Hasse de quatro relações de ordem sobre o conjunto $\{1, 2, 3, 4, 5\}$. Na relação \mathcal{R}_1 , o único elemento minimal é 3, e os elementos maximais são 1, 4 e 5. Na relação \mathcal{R}_2 , os elementos minimais são 3 e 5, e o único maximal é 4. Na relação \mathcal{R}_3 , o único minimal é 2 e o único maximal é 4. Na relação \mathcal{R}_4 os minimais são 3 e 5, e os maximais são 2 e 4.

Os conceitos de minimal e maximal são muito usados quando A é um conjunto de conjuntos, e \mathcal{R} é a relação ‘ \subseteq ’. Neste caso, um elemento minimal de A é um conjunto que não contém propriamente nenhum outro elemento de A . Por exemplo, seja

$$A = \{\{2\}, \{1, 2\}, \{1, 3\}, \{1, 2, 4\}, \{3, 4, 5\}\}$$

Neste conjunto, o elemento $\{1, 2, 4\}$ não é minimal, pois ele contém propriamente o conjunto $\{1, 2\}$ que também está em A . Por outro lado, $\{2\}$, $\{1, 3\}$, e $\{3, 4, 5\}$ são minimais sob a relação ‘ \subseteq ’. Analogamente o elemento $\{2\}$ não é maximal pois $\{2\} \subseteq \{1, 2, 4\}$. Os elementos maximais de A sob \subseteq são $\{1, 3\}$, $\{1, 2, 4\}$ e $\{3, 4, 5\}$.

Exercício 6.36: Encontre os elementos minimais e maximais em cada uma das relações da figura 6.4.

Exercício 6.37: Encontre um conjunto A e uma relação de ordem \mathcal{R} sobre A tal que existe um único elemento minimal em A sob \mathcal{R} , mas que não é mínimo.

Exercício 6.38: Seja $A = \{3, 6, 9, \dots\}$ o conjunto dos múltiplos positivos de 3, e \mathcal{R} a relação sobre A tal que (x, y) está em \mathcal{R} se e somente se todos os algarismos decimais de x aparecem em y , na mesma sequência. Assim, por exemplo, $(262, 12682)$ está em \mathcal{R} , mas $(262, 12268)$ não está. Determine os elementos minimais de A sob \mathcal{R} .

Exercício 6.39: Seja $A = \{X \subseteq \mathbb{N} : X \neq \emptyset \wedge |X| \text{ é par}\}$. Note que A não é um conjunto de inteiros, mas sim um conjunto de conjuntos: $\{1, 2, 3, 4\}$ e $\{10, 20\}$ são elementos de A , enquanto que 20 e $\{20, 40, 60\}$ não são. Seja \mathcal{R} a relação “ \subseteq ” de continência de conjuntos. Encontre os elementos minimais de A sob \mathcal{R} . Existe algum elemento maximal de A sob \mathcal{R} ?

Exercício 6.40: Seja $\mathcal{R} = \{(x, y) \in N - \{0\} \times N - \{0\} : x \text{ divide } y\}$.

1. Prove que \mathcal{R} é uma relação de ordem definida sobre $N - \{0\}$.
2. A relação de ordem \mathcal{R} é total? Prove ou dê um contra-exemplo.
3. Quais são os elementos minimais de $N - \{0\}$ sob \mathcal{R} ?
4. O conjunto $N - \{0\}$ tem um elemento mínimo sob \mathcal{R} ?

6.7 Relações de equivalência

Definição 6.5: Uma *relação de equivalência sobre* um conjunto A é uma relação \mathcal{R} sobre A que é reflexiva sobre A , simétrica e transitiva.

Exemplo 6.39: Seja A o conjunto de todas as retas do plano, e seja \mathcal{R} a relação $X\mathcal{R}Y$ se, e somente se, $X = Y$ ou $X \cap Y = \emptyset$. Esta relação é simplesmente a relação de paralelismo da geometria plana. Claramente a relação é reflexiva sobre A , simétrica e transitiva, logo é uma relação de equivalência.

Exemplo 6.40: Sejam \mathbb{Z} o conjunto dos números inteiros. A relação

$$\mathcal{R} = \{(a, b) : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (a - b) \text{ é múltiplo de } 5\}$$

é uma relação de equivalência. Verificando:

- \mathcal{R} é reflexiva sobre \mathbb{Z} : para todo $a \in \mathbb{Z}$, temos $(a, a) \in \mathcal{R}$, pois $a - a = 0 \cdot 5$.
- \mathcal{R} é simétrica: para todo $(a, b) \in \mathcal{R}$, temos $a - b = 5r$ para algum $r \in \mathbb{Z}$; logo $b - a = 5(-r)$, portanto $(b, a) \in \mathcal{R}$.
- \mathcal{R} é transitiva: para todo $(a, b) \in \mathcal{R}$ e todo $(b, c) \in \mathcal{R}$, temos $a - b = 5r$ para algum $r \in \mathbb{Z}$, e $b - c = 5s$ para algum $s \in \mathbb{Z}$; logo $c = b - 5s$, $a - c = a - b + 5s = 5r + 5s = 5(r + s)$; portanto $(a, c) \in \mathcal{R}$.

No exemplo 6.40 o número 5 pode ser substituído por qualquer inteiro m . Esta relação é denominada *congruência módulo m* .

Exemplo 6.41: Para todo conjunto A , a relação de identidade I_A é uma relação de equivalência sobre A .

Exemplo 6.42: Para todo conjunto A , o produto cartesiano $A \times A$ é uma relação de equivalência sobre A (onde quaisquer dois elementos estão relacionados entre si).

Exemplo 6.43: Seja A um conjunto não vazio. A relação \subseteq entre os conjuntos de $\mathbb{P}(A)$ é reflexiva sobre $\mathbb{P}(A)$ e transitiva, mas não é uma relação de equivalência sobre $\mathbb{P}(A)$, pois ela não é simétrica (por exemplo, $\emptyset \subseteq A$ mas $A \not\subseteq \emptyset$).

Se \mathcal{R} é uma relação de equivalência, a notação $a\mathcal{R}b$ também pode ser lida “ a é equivalente a b módulo \mathcal{R} ,” e denotada por $a \equiv b \pmod{\mathcal{R}}$. Analogamente, $a\not\mathcal{R}b$ pode ser lida “ a não é equivalente a b módulo \mathcal{R} ,” e denotada por $a \not\equiv b \pmod{\mathcal{R}}$.

6.7.1 Classes de equivalência

Seja \mathcal{R} uma relação de equivalência sobre um conjunto A . Para todo elemento $a \in A$, o conjunto

$$[a]_{\mathcal{R}} = \{x \in A : x\mathcal{R}a\}$$

é denominado a *classe de equivalência* do elemento a .

Exemplo 6.44: Vamos construir as classes de equivalência da relação \mathcal{R} de congruência módulo 5 (exemplo 6.40).

A classe de equivalência de um inteiro i , é o conjunto

$$[i]_{\mathcal{R}} = \{x \in \mathbb{Z} : (\exists s \in \mathbb{Z}) x - i = 5s\}$$

Ou seja, $x \in [i]_{\mathcal{R}}$ se e somente se $x = 5k + i$ para algum $r \in \mathbb{Z}$; isto é, se e somente se x tem o mesmo resto que i quando dividido por 5. Portanto existem apenas 5 classes de equivalência, que correspondem aos possíveis restos da divisão por 5:

- $[0]_{\mathcal{R}} = \{\dots, -10, -5, 0, 5, 10, \dots\}$.
- $[1]_{\mathcal{R}} = \{\dots, -9, -4, 1, 6, 11, \dots\}$.
- $[2]_{\mathcal{R}} = \{\dots, -8, -3, 2, 7, 12, \dots\}$.
- $[3]_{\mathcal{R}} = \{\dots, -7, -2, 3, 8, 13, \dots\}$.
- $[4]_{\mathcal{R}} = \{\dots, -6, -1, 4, 9, 14, \dots\}$.

Teorema 6.7: Seja \mathcal{R} uma relação de equivalência sobre um conjunto A . As seguintes afirmações são equivalentes.

- $a\mathcal{R}b$.
- $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.

- $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$

Prova:

- Vamos provar que $a\mathcal{R}b \rightarrow [a]_{\mathcal{R}} = [b]_{\mathcal{R}}$. Seja c um elemento qualquer de $[a]_{\mathcal{R}}$. Por definição, $c\mathcal{R}a$. Como \mathcal{R} é uma relação de equivalência, se $a\mathcal{R}b$ então $c\mathcal{R}b$ (por transitividade), e portanto $c \in [b]_{\mathcal{R}}$. Concluimos assim que $[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}}$. Analogamente prova-se que $[b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}$. Portanto $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$.
- Vamos provar que $[a]_{\mathcal{R}} = [b]_{\mathcal{R}} \rightarrow [a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$. Se $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$, então $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = [a]_{\mathcal{R}} \cap [a]_{\mathcal{R}} = [a]_{\mathcal{R}}$. Como \mathcal{R} é reflexiva sobre A , temos $a \in [a]_{\mathcal{R}}$, logo $[a]_{\mathcal{R}} \neq \emptyset$. Concluimos que $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$.
- Vamos provar que $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset \rightarrow a\mathcal{R}b$. Como $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} \neq \emptyset$ então existe um $c \in A$ tal que $c \in [a]_{\mathcal{R}}$ e $c \in [b]_{\mathcal{R}}$. Por definição, $c\mathcal{R}a$ e $c\mathcal{R}b$. Por simetria e transitividade de \mathcal{R} , concluimos que $a\mathcal{R}b$.

Fim.

Cada elemento de uma classe de equivalência é chamado de uma *representante* dessa classe. Ou seja, para qualquer $a \in A$, qualquer elemento $b \in A$ equivalente a a módulo \mathcal{R} tem a mesma classe de equivalência que a , e portanto pode ser usado como um representante da classe $[a]_{\mathcal{R}}$.

6.7.2 Relações de equivalência e partições

O que o teorema 6.7 nos mostra é as que classes de uma relação de equivalência \mathcal{R} sobre um conjunto A são duas a duas disjuntas. Como todo elemento de A está em alguma classe, a união de todas as classes é o conjunto A . Isto significa que as classes de equivalência de \mathcal{R} formam uma partição do conjunto A . (Veja a seção 2.9.)

Vamos mostrar agora que toda partição de um conjunto pode ser usada para construir uma relação de equivalência sobre esse conjunto. Dizemos que dois elementos estão relacionados se e somente se eles estão no mesmo bloco da partição. Mais precisamente:

Teorema 6.8: Sejam P uma partição do conjunto A , e S_P a relação

$$S_P = \{(x, y) : (\exists C \in P) x \in C \wedge y \in C\}.$$

Então S_P é uma relação de equivalência, e suas classes são os blocos da partição P .

Prova:

Para mostrar que S_P é uma relação de equivalência, precisamos mostrar que ela é reflexiva sobre A , simétrica e transitiva.

- A relação é reflexiva sobre A : para todo $a \in A$, temos aS_Pa ; pois, pela definição de partição, todo elemento de A pertence a algum bloco C da partição P .
- A relação é simétrica: para todo $(a, b) \in S_P$, por definição a e b pertencem a algum sub-conjunto $C \in P$; logo bS_Pa .

- A relação é transitiva: para quaisquer (a, b) e (b, c) em \mathcal{S}_P , existem blocos C e D de P tais que $a, b \in C$ e $b, c \in D$; logo $b \in C \cap D$. Como os blocos de uma partição são disjuntos dois a dois, concluímos que C e D são o mesmo bloco. Portanto a e c pertencem ao mesmo bloco, logo $a\mathcal{S}_P c$.

Fim.

Exercício 6.41: Seja $\mathcal{S} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Q}\}$. Mostre que \mathcal{S} é uma relação de equivalência.

Exercício 6.42: Seja \mathcal{R} uma relação sobre o conjunto dos pares ordenados de inteiros positivos definida por $((a, b)\mathcal{R}(c, d))$ se, e somente se, $ad = bc$.

1. Prove que \mathcal{R} é uma relação de equivalência.
2. Descreva a classe de equivalência de $(1, 2)$ segundo a relação \mathcal{R} .

Exercício 6.43: Seja ε um número real positivo, e considere a relação \approx_ε sobre \mathbb{R} tal que

$$x \approx_\varepsilon y \leftrightarrow |x - y| \leq \varepsilon$$

para quaisquer x e y em \mathbb{R} . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

Exercício 6.44: Considere a relação \mathcal{R} sobre os pares ordenados de inteiros $\mathbb{Z} \times \mathbb{Z}$ tal que

$$(a, b)\mathcal{R}(c, d) \leftrightarrow ((a = c) \wedge (b = d)) \vee ((a = d) \wedge (b = c))$$

para quaisquer inteiros a, b, c e d . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

Capítulo 7

Funções, sequências e relações n -árias

7.1 Funções

7.1.1 Conceito

Definição 7.1: Dizemos que uma relação \mathcal{F} de A para B é uma *função de A para B* se, e somente se, para todo $a \in A$ existe exatamente um $b \in B$ tal que $(a, b) \in \mathcal{F}$.

Portanto, como vimos na seção 6.1, uma função \mathcal{F} de A para B é um subconjunto do produto cartesiano $A \times B$, ou seja um conjunto de pares (a, b) com $a \in A$ e $b \in B$, com a propriedade acima.

Para indicar que \mathcal{F} é uma função de A para B , usa-se geralmente a notação $\mathcal{F} : A \rightarrow B$. Para cada elemento a de A , é costume indicar por $\mathcal{F}(a)$ o *valor de \mathcal{F} em a* , isto é, o único elemento b de B tal que $(a, b) \in \mathcal{F}$. Observe que esta notação só tem sentido para funções, e não para relações em geral.

Exemplo 7.1: A relação $\mathcal{F} = \{(1, 40), (2, 30), (3, 30)\}$ é uma função do conjunto $X = \{1, 2, 3\}$ para o conjunto $Y = \{20, 30, 40\}$, isto é $\mathcal{F} : X \rightarrow Y$.

Exemplo 7.2: A relação $\mathcal{F} = \{(1, 40), (3, 30)\}$ *não* é uma função de $X = \{1, 2, 3\}$ para $Y = \{20, 30, 40\}$, pois para $a = 2 \in X$ *não* existe um $b \in Y$ tal que $(a, b) \in \mathcal{F}$.

Exemplo 7.3: A relação $\mathcal{F} = \{(1, 40), (2, 20), (2, 30), (3, 30)\}$ *não* é uma função de $X = \{1, 2, 3\}$ para $Y = \{20, 30, 40\}$, pois para $a = 2 \in X$ existem *dois* valores distintos $b' = 20 \in Y$ e $b'' = 30 \in Y$ tais que $(a, b') \in \mathcal{F}$ e $(a, b'') \in \mathcal{F}$.

Exemplo 7.4: A relação $\mathcal{F} = \{(x, x^2) : x \in \mathbb{Z}\}$ é uma função do conjunto \mathbb{Z} para o conjunto \mathbb{N} , isto é $\mathcal{F} : \mathbb{Z} \rightarrow \mathbb{N}$.

Exemplo 7.5: A relação $\mathcal{F} = \{(x^2, x) : x \in \mathbb{Z}\}$ *não* é uma função do conjunto \mathbb{N} para o conjunto \mathbb{Z} , pois há elementos $a \in \mathbb{N}$ (como $a = 5$) para os quais não existe par $(a, b) \in \mathcal{F}$, e há elementos $a \in \mathbb{N}$ (como $a = 4$) para os quais existem dois pares $(a, b) \in \mathcal{F}$ (no caso, $(4, 2)$ e $(4, -2)$).

7.1.2 Domínio e imagem de uma função

Uma vez que funções são um tipo particular de relações, todos os conceitos introduzidos para relações (como domínio, composição, inversa, etc.) valem também para funções. Por exemplo se \mathcal{F} é uma função de A para B , então, de acordo com a definição, o domínio $\text{Dom}(\mathcal{F})$ de \mathcal{F} é sempre o conjunto A .

A imagem ou contra-domínio $\text{Img}(\mathcal{F})$ de \mathcal{F} é o conjunto

$$\text{Img}(\mathcal{F}) = \{\mathcal{F}(a) : a \in A\} = \{b \in B : (\exists a \in A) b = \mathcal{F}(a)\}$$

Observe que a imagem está contida no conjunto B , mas nem sempre é igual a B .

Podemos portanto dizer que duas funções $\mathcal{F} : A \rightarrow B$ e $\mathcal{G} : C \rightarrow D$ são a mesma função se, e somente se, $A = C$, e $(\forall a \in A) \mathcal{F}(a) = \mathcal{G}(a)$.

Como observamos no caso de relações em geral, se \mathcal{F} é uma função de A para B , e $B \subseteq C$, então \mathcal{F} também é uma função de A para C . Por exemplo, a função *seno* é uma função do conjunto dos números reais \mathbb{R} para o intervalo $B = [-1, +1]$. Como B é um subconjunto de \mathbb{R} , então *seno* também é uma função de \mathbb{R} para \mathbb{R} .

Porém, precisamos observar que alguns autores consideram que o conjunto B é parte da definição da função. Nesta abordagem, se \mathcal{F} for definida como função de A para B , e C for um conjunto diferente de B , então \mathcal{F} não é uma função de A para C . Para esses autores, por exemplo, *seno* pode ser definida como função de \mathbb{R} para \mathbb{R} , ou de \mathbb{R} para $[-1, +1]$; mas estas duas escolhas resultam em funções distintas. Neste livro não seguimos essa abordagem: para nós, uma função, assim como uma relação, é apenas o conjunto dos seus pares.

7.1.3 As funções piso e teto

Em álgebra e cálculo são estudados muitos exemplos de funções, como raiz quadrada, seno, cosseno, logaritmo, etc. A seguir veremos duas funções que são especialmente importantes em computação.

Definição 7.2: A *função piso* (também chamada de *chão* ou *solo*) associa a cada número real x o maior inteiro que é menor ou igual a x . Este inteiro é denotado por $\lfloor x \rfloor$.

Observe que $\lfloor 1/3 \rfloor = \lfloor 2/3 \rfloor = 0$, $\lfloor -1/3 \rfloor = \lfloor -2/3 \rfloor = -1$ e $\lfloor 5 \rfloor = 5$.

Definição 7.3: A *função teto* associa a cada número real x o menor inteiro que é maior ou igual a x . Este inteiro denotado por $\lceil x \rceil$.

Observe que $\lceil 5/4 \rceil = \lceil 7/4 \rceil = 2$, $\lceil -1/4 \rceil = \lceil -3/4 \rceil = 0$ e $\lceil 4 \rceil = 4$

Tanto o piso quanto o teto são funções do conjunto \mathbb{R} para o conjunto \mathbb{Z} . Essas funções tem algumas propriedades importantes:

- $\lfloor x \rfloor = n$ se, e somente se $n \leq x < n + 1$.
- $\lfloor x \rfloor = n$ se, e somente se $x - 1 < n \leq x$.
- $\lceil x \rceil = n$ se, e somente se $n - 1 < x \leq n$.

- $\lceil x \rceil = n$ se, e somente se $x \leq n < x + 1$.
- $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$.
- $\lfloor -x \rfloor = -\lceil x \rceil$.
- $\lceil -x \rceil = -\lfloor x \rfloor$.

Exercício 7.1: Sejam A e B conjuntos finitos com $|A| = n$ e $|B| = m$. Quantas funções poderão ser definidas de A para B ?

Exercício 7.2: Prove que $\lceil x + n \rceil = \lceil x \rceil + n$ e $\lfloor x + n \rfloor = \lfloor x \rfloor + n$.

Exercício 7.3: Prove, ou dê um contra exemplo, que $\lceil x + y \rceil = \lceil x \rceil + y$ e $\lfloor x + y \rfloor = \lfloor x \rfloor + y$.

Exercício 7.4: Seja ε um número real positivo, e considere a relação \sim_ε sobre \mathbb{R} tal que

$$x \sim_\varepsilon y \leftrightarrow \left\lfloor \frac{x}{\varepsilon} \right\rfloor = \left\lfloor \frac{y}{\varepsilon} \right\rfloor$$

para quaisquer x e y em \mathbb{R} . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

7.1.4 Função injetora, sobrejetora e bijetora

Definição 7.4: Uma função \mathcal{F} de A para B é *injetora* se, e somente se, $(\forall x, y \in A) (\mathcal{F}(x) = \mathcal{F}(y) \rightarrow (x = y))$.

Ou seja, \mathcal{F} é injetora se e somente se ela atribui um valor diferente para cada elemento do domínio.

Diz-se também que estas funções *preservam informação*, pois o valor de $\mathcal{F}(x)$ determina unicamente o valor de x . Funções injetoras também são chamadas de funções *um para um*.

Exercício 7.5: Sejam A e B conjuntos finitos com m e n elementos, respectivamente. Quantas funções injetoras $\mathcal{F} : A \rightarrow B$ existem?

Exercício 7.6: Sejam $f : A \rightarrow B$ e $g : B \rightarrow C$. Prove que se $g \circ f : A \rightarrow C$ não é injetora então pelo menos uma dentre f e g é não injetora.

Exercício 7.7: Sejam $\mathcal{F} : A \rightarrow C$ e $\mathcal{G} : B \rightarrow D$ duas funções injetoras. Considere a função:

$$\begin{aligned} \mathcal{H} : A \times B &\rightarrow C \times D \\ \mathcal{H}(a, b) &\rightarrow (\mathcal{F}(a), \mathcal{G}(b)) \end{aligned}$$

Prove que \mathcal{H} é uma função injetora.

Definição 7.5: Uma função \mathcal{F} de A para B é *sobrejetora em B* (ou é uma função de A sobre B) se, e somente se, $(\forall b \in B) (\exists a \in A) \mathcal{F}(a) = b$.

Ou seja \mathcal{F} é uma função sobre B se e somente se $B = \text{Im}(\mathcal{F})$. Note que não tem sentido dizer que uma função “é sobrejetora” sem especificar em qual conjunto. Por exemplo, a função piso é tanto uma função de \mathbb{R} para \mathbb{Z} quanto de \mathbb{R} para \mathbb{R} ; ela é sobrejetora em \mathbb{Z} , mas não em \mathbb{R} .

Exercício 7.8: Sejam A e B conjuntos finitos com m e n elementos, respectivamente. Quantas funções sobrejetoras $\mathcal{F} : A \rightarrow B$ existem?

Definição 7.6: Uma função \mathcal{F} de A para B é *bijetora de A para B* (ou é uma *bijeção de A para B*) se, e somente se, \mathcal{F} é injetora e sobrejetora em B .

Dito de outra forma, uma relação \mathcal{F} é uma bijeção se A para B se, e somente se, $(\forall a \in A)(\exists! b \in B)(\mathcal{F}(a) = b)$ (isto é, \mathcal{F} é uma função de A para B), e $(\forall b \in B)(\exists! y \in A)(\mathcal{F}(y) = b)$.

Funções bijetoras são muito importantes em matemática e computação. Entre outras coisas, elas permitem definir o “tamanho” de conjuntos infinitos, como veremos no capítulo 11.

Exercício 7.9: Sejam A e B conjuntos finitos com m e n elementos, respectivamente. Quantas funções bijetoras de A para B existem?

Exercício 7.10: Seja A um conjunto finito com n elementos. Quantas funções bijetoras de A para A existem?

Exercício 7.11: Sejam A e B dois conjuntos não vazios. Considere a função $\mathcal{P} : A \times B \rightarrow A$ onde $\mathcal{P}((a, b)) = a$. Prove as afirmações abaixo ou dê um contra-exemplo.

1. A função \mathcal{P} é uma função sobrejetora.
2. A função \mathcal{P} é uma função bijetora.

7.1.5 Composição de funções

Uma vez que funções são relações, a composição de duas funções \mathcal{F} e \mathcal{G} é definida da mesma forma que para relações, ou seja, é a relação

$$\mathcal{G} \circ \mathcal{F} = \{ (a, c) : (\exists b) (a, b) \in \mathcal{F} \wedge (b, c) \in \mathcal{G} \}$$

Em particular, se $\mathcal{F} : A \rightarrow B$ e $\mathcal{G} : B \rightarrow C$, então verifica-se que $\mathcal{G} \circ \mathcal{F}$ é uma função de A para C , e para todo $a \in A$ o valor de $\mathcal{G} \circ \mathcal{F}$ em a é definido pela fórmula:

$$(\mathcal{G} \circ \mathcal{F})(a) = \mathcal{G}(\mathcal{F}(a))$$

Por exemplo, sejam $\mathcal{F} : \mathbb{R} \rightarrow \mathbb{R}$ com $\mathcal{F}(x) = 2x + 3$, e $\mathcal{G} : \mathbb{R} \rightarrow \mathbb{R}$ com $\mathcal{G}(x) = 3x + 2$. Então $(\mathcal{G} \circ \mathcal{F})(x) = \mathcal{G}(\mathcal{F}(x)) = \mathcal{G}(2x + 3) = 3(2x + 3) + 2 = 6x + 11$ e $(\mathcal{F} \circ \mathcal{G})(x) = \mathcal{F}(\mathcal{G}(x)) = \mathcal{F}(3x + 2) = 2(3x + 2) + 3 = 6x + 7$. Este exemplo mostra que a composição de funções não é comutativa.

Na verdade, demonstra-se que a composição de duas funções quaisquer é sempre uma função. Como vimos na seção 6.2, é também verdade que

$$\text{Dom}(\mathcal{G} \circ \mathcal{F}) \subseteq \text{Dom}(\mathcal{F})$$

e

$$\text{Img}(\mathcal{G} \circ \mathcal{F}) \subseteq \text{Img}(\mathcal{G})$$

Além disso, no caso de funções, temos que

$$\text{Img}(\mathcal{F}) \subseteq \text{Dom}(\mathcal{G}) \Leftrightarrow \text{Dom}(\mathcal{G} \circ \mathcal{F}) = \text{Dom}(\mathcal{F})$$

e

$$\text{Dom}(\mathcal{G}) \subseteq \text{Img}(\mathcal{F}) \Leftrightarrow \text{Img}(\mathcal{G} \circ \mathcal{F}) = \text{Img}(\mathcal{G})$$

Exemplo 7.6: Seja \mathcal{F} a função logaritmo, $\mathcal{F}(x) = \log x$, \mathcal{G} a função raiz quadrada, $\mathcal{G}(y) = \sqrt{y}$. Seja \mathbb{R}^+ o conjunto de todos os reais não negativos.

$$\begin{aligned} \text{Dom}(\mathcal{F}) &= \mathbb{R}^+ \setminus \{0\} & \text{Dom}(\mathcal{G}) &= \mathbb{R}^+ \\ \text{Img}(\mathcal{F}) &= \mathbb{R} & \text{Img}(\mathcal{G}) &= \mathbb{R}^+ \end{aligned}$$

Observe que a imagem de \mathcal{F} não está contida no domínio de \mathcal{G} . A composição $\mathcal{G} \circ \mathcal{F}$ é a raiz quadrada do logaritmo, $(\mathcal{G} \circ \mathcal{F})(x) = \sqrt{\log x}$. O domínio desta função não é $\text{Dom}(\mathcal{F})$, mas o conjunto dos números reais maiores ou iguais a 1, que é subconjunto próprio de $\text{Dom}(\mathcal{F})$. Por outro lado, a imagem de $\mathcal{G} \circ \mathcal{F}$ é \mathbb{R}^+ , que neste exemplo é igual a $\text{Img}(\mathcal{G})$.

Exemplo 7.7: Sejam \mathcal{F} e \mathcal{G} as funções logaritmo e raiz quadrada, como no exemplo 7.6. A composição $\mathcal{F} \circ \mathcal{G}$ é o logaritmo da raiz quadrada, $(\mathcal{F} \circ \mathcal{G})(y) = \log \sqrt{y}$; como $\text{Img}(\mathcal{F}) \subseteq \text{Dom}(\mathcal{G})$, então $\text{Dom}(\mathcal{F} \circ \mathcal{G}) = \text{Dom}(\mathcal{G}) = \mathbb{R}^+$; e como $\text{Dom}(\mathcal{F}) \subseteq \text{Img}(\mathcal{G})$, $\text{Img}(\mathcal{F} \circ \mathcal{G}) = \text{Img}(\mathcal{F}) = \mathbb{R}$.

Teorema 7.1: Sejam $\mathcal{F} : A \rightarrow B$, $\mathcal{G} : B \rightarrow C$ e $\mathcal{G} \circ \mathcal{F} : A \rightarrow C$ então:

- se \mathcal{F} e \mathcal{G} são injetoras então $\mathcal{G} \circ \mathcal{F}$ é injetora.
- se \mathcal{F} é sobrejetora em B , e \mathcal{G} é sobrejetora em C , então $\mathcal{G} \circ \mathcal{F}$ é sobrejetora em C .

Exercício 7.12: Demonstre o teorema 7.1.

7.1.6 Função inversa

A inversa de uma função \mathcal{F} é definida como na seção 6.1.4, ou seja, é a relação

$$\mathcal{F}^{-1} = \{ (y, x) : (x, y) \in \mathcal{F} \}$$

Se \mathcal{F} é uma bijeção do conjunto A para o conjunto B , então verifica-se que a inversa \mathcal{F}^{-1} também é uma função, do conjunto B para o conjunto A , tal que, para todo a em A e todo b em B , $(\mathcal{F}^{-1}(b) = a) \leftrightarrow (\mathcal{F}(a) = b)$. Portanto,

$$(\forall a \in A) \mathcal{F}^{-1}(\mathcal{F}(a)) = a$$

$$(\forall b \in B) \mathcal{F}(\mathcal{F}^{-1}(b)) = b$$

Dito de outra forma, \mathcal{F} é uma bijeção de A para B se, e somente se, $\mathcal{F}^{-1} \circ \mathcal{F} = I_A$ e $\mathcal{F} \circ \mathcal{F}^{-1} = I_B$. Observe que a inversa de uma bijeção de A para B também é uma bijeção de B para A .

Exercício 7.13: Seja \mathcal{F} uma função. Prove que a relação \mathcal{F}^{-1} também é uma função se e somente se \mathcal{F} é injetora.

7.1.7 Imagem e imagem inversa de conjuntos

Para qualquer função \mathcal{F} e qualquer conjunto X , verifica-se que a imagem de X sob \mathcal{F} , definida na seção 6.1.5, é

$$\mathcal{F}(X) = \{\mathcal{F}(x) : x \in (X \cap \text{Dom}(\mathcal{F}))\} = \{y \in \text{Img}(\mathcal{F}) : (\exists x \in X) \mathcal{F}(x) = y\}$$

Note que os elementos de X que não estão em $\text{Dom}(\mathcal{F})$ não contribuem para a imagem. Este conceito é geralmente usado quando $X \subseteq \text{Dom}(\mathcal{F})$. A imagem inversa de um conjunto Y qualquer sob \mathcal{F} , também definida na seção 6.1.5, é a imagem de Y sob a relação inversa \mathcal{F}^{-1} , ou seja

$$\mathcal{F}^{-1}(Y) = \{x \in \text{Dom}(\mathcal{F}) : \mathcal{F}(x) \in Y\} = \{x \in \text{Dom}(\mathcal{F}) : (\exists y) (x, y) \in \mathcal{F}\}$$

Observe que a função \mathcal{F} pode não ser injetora e nem sobrejetora, e portanto \mathcal{F}^{-1} pode não ser uma função. Isto não é um problema uma vez que os conceitos de imagem e imagem inversa são definidos para relações em geral.

7.1.8 Restrição de funções

O conceito de restrição de relações pode ser aplicado também a funções. Se \mathcal{F} é uma função e X é um conjunto, a notação $\mathcal{F}|X$ ou $\mathcal{F}|_X$ é frequentemente usada para indicar a restrição de \mathcal{F} (vista como relação) aos conjuntos X e $\text{Img}(\mathcal{F})$. Isto é,

$$\mathcal{F}|X = \mathcal{F} \cap (X \times \text{Img}(\mathcal{F})) = \{(x, y) : (x, y) \in \mathcal{F} \wedge x \in X\}$$

Este conceito também é geralmente usado quando X é um subconjunto de $\text{Dom}(\mathcal{F})$.

Exercício 7.14: Sejam \mathcal{F} uma função, e A, B subconjuntos de $\text{Dom}(\mathcal{F})$. Prove que $\mathcal{F}(A \cap B) \subseteq \mathcal{F}(A) \cap \mathcal{F}(B)$. Mais ainda, se \mathcal{F} é injetora então $\mathcal{F}(A \cap B) = \mathcal{F}(A) \cap \mathcal{F}(B)$.

Exercício 7.15: Sejam \mathcal{F} uma função, A, B subconjuntos de $\text{Dom}(\mathcal{F})$ e U, V subconjuntos de $\text{Img}(\mathcal{F})$. Prove ou encontre contra-exemplos para cada uma destas afirmações:

- $\mathcal{F}(A \cup B) = \mathcal{F}(A) \cup \mathcal{F}(B)$.
- $\mathcal{F}(A \setminus B) = \mathcal{F}(A) \setminus \mathcal{F}(B)$.
- $B \subseteq A \leftrightarrow \mathcal{F}(B) \subseteq \mathcal{F}(A)$.
- $\mathcal{F}^{-1}(U \cap V) = \mathcal{F}^{-1}(U) \cap \mathcal{F}^{-1}(V)$.
- $\mathcal{F}^{-1}(U \cup V) = \mathcal{F}^{-1}(U) \cup \mathcal{F}^{-1}(V)$.
- $\mathcal{F}^{-1}(U \setminus V) = \mathcal{F}^{-1}(U) \setminus \mathcal{F}^{-1}(V)$.
- $U \subseteq V \leftrightarrow \mathcal{F}^{-1}(U) \subseteq \mathcal{F}^{-1}(V)$.
- $\mathcal{F}^{-1}(\mathcal{F}(A)) = A$.
- $\mathcal{F}(\mathcal{F}^{-1}(U)) = U$.

Exercício 7.16: Seja \mathcal{F} uma função de um conjunto A para um conjunto B . Considere a relação \mathcal{R} sobre A tal que

$$a\mathcal{R}b \leftrightarrow \mathcal{F}(a) = \mathcal{F}(b)$$

para quaisquer elementos a e b de A . Esta é uma relação de equivalência? Em caso afirmativo, descreva suas classes de equivalência.

7.1.9 Permutações

Uma *permutação* de um conjunto A é uma função bijetora de A para A . Observe que a relação de identidade sobre A é uma permutação (trivial) de A .

Por ser bijetora, toda permutação de um conjunto A tem uma inversa, que é uma permutação de A . A composição de duas permutações de A é uma permutação de A .

Uma permutação f de um conjunto A pode ser interpretada como uma maneira de colocar os elementos de A em um conjunto de caixas, cada uma rotulada com um elemento de A . Ou seja, a permutação f estaria dizendo que o elemento x de A está na caixa de rótulo $f(x)$. Ou, alternativamente, que a caixa de rótulo x contém o elemento $f(x)$.

Uma permutação f também pode ser entendida como uma maneira de trocar o conteúdo de uma coleção de caixas rotuladas com elementos de A . Nesse caso, para cada x em A , o elemento na caixa de rótulo x deve ser transferido para a caixa de rótulo $f(x)$. Ou então, a caixa de rótulo x deve receber o conteúdo da caixa de rótulo $f(x)$. Nas duas interpretações, entende-se que todas as trocas são realizadas simultaneamente.

Permutações são muito importantes em computação. Por exemplo a ordenação dos elementos de uma lista de n elementos, ou dos n registros de um arquivo, pode ser vista como a aplicação de uma permutação dos índices $\{0..n-1\}$.

Um *elemento fixo* de uma função f é um elemento $x \in \text{Dom } f$ tal que $f(x) = x$. Note que uma permutação que não é a identidade ainda pode ter um ou mais elementos fixos. O nome *desarranjo* é ocasionalmente usado para permutações que não tem nenhum elemento fixo.

Exercício 7.17: Liste todas as permutações do conjunto $A = \{10, 20, 30\}$.

Exercício 7.18: Liste todas as permutações do conjunto $A = \{10, 20, 30, 40\}$.

Exercício 7.19: Quantas permutações existem do conjunto $A = \{1, 2, 3, 4, 5, 6\}$.

Exercício 7.20: Considere uma caixa quadrada de papelão com tampa. Suponha que os lados da caixa e da tampa são rotulados em ordem anti-horária com inteiros de 0 a 4. Cada maneira de fechar a caixa com a tampa corresponde a uma permutação f do conjunto $A = \{0, 1, 2, 3\}$, tal que $f(k)$ é o lado da tampa que é encaixado sobre o lado k da caixa, para cada k em A . Escreva as permutações de A que correspondem a todos os jeitos possíveis de tampar a caixa.

Exercício 7.21: Um dado de jogar tem as faces numeradas de 1 a 6, de tal modo tal que faces opostas somam 7. Suponha que o dado é rodado de modo que ele termina na mesma posição onde começou, exceto que algumas faces podem ficar trocadas entre si. A rotação pode ser descrita por uma permutação f do conjunto $A = \{1, 2, 3, 4, 5, 6\}$, tal que a face k termina onde estava a face $f(k)$.

1. Liste todas as permutações de A que podem ser obtidas desta forma.
2. Se f e g são duas dessas permutações, qual é o significado da composição $f \circ g$? Ela também é uma dessas permutações?

7.1.10 Funções idempotentes

Uma função f é dita *idempotente* se a composição $f \circ f$ é igual a f . Ou seja, se $f(f(x)) = f(x)$ para todo $x \in \text{Dom}(f)$. Esta condição também equivale a dizer que f restrita a $\text{Img}(f)$ é a função identidade sobre $\text{Img}(f)$.

Por exemplo, as funções solo e teto definidas na seção 7.1.3 são idempotentes. Outro exemplo é a função f com domínio $\mathbb{N} \setminus \{0, 1\}$ tal que $f(z)$ é o menor fator primo de z .

Exercício 7.22: Prove que a composição de duas funções idempotentes é uma função idempotente.

Em álgebra linear, uma transformação linear idempotente é chamada de *projeção*.

7.2 Sequências finitas

Uma *sequência finita* é uma função x cujo domínio é um intervalo de inteiros $\{n \in \mathbb{Z} : r \leq n \leq s\}$, onde r e s são inteiros; que pode ser abreviado para $\{r..s\}$. Se os valores de x pertencem a um conjunto A , dizemos que x é uma sequência finita *sobre* A . Em algumas áreas da matemática e da computação, sequências finita também são chamadas de *listas*, *palavras*, *ênuplas* ou *cadeias*.

A imagem de um inteiro n por uma sequência x é habitualmente denotada por x_n (em vez de $x(n)$). Os pares (n, x_n) são os *termos* ou *elementos* da sequência; o inteiro n é o *índice* do termo, e x_n é seu *valor*. Os inteiros r e s são o *índice inicial* e o *índice final* da sequência.

Exemplo 7.8: Seja $x : \{2..6\} \rightarrow \mathbb{R}$ cujos termos são $\{(2, 4), (3, 9), (4, 16), (5, 25), (6, 36)\}$. Podemos então escrever que $x_2 = 4$, $x_3 = 9$, e $x_n = n^2$ para todo $n \in \{2..6\}$.

Note que uma sequência especifica não apenas os valores dos termos mas também sua ordem e seus índices. Note também que uma sequência pode ter mais de um termo com o mesmo valor. Duas sequências são iguais se, e somente se, elas tem exatamente os mesmos termos — mesmos índices e mesmos valores.

7.2.1 Notação para sequências finitas

Quando o índice inicial r é especificado pelo contexto, uma sequência finita é geralmente denotada colocando-se os valores dos termos entre parênteses e separados por vírgulas. Por exemplo, se convencionamos que os índices começam com zero, a notação $(1, 2, 2, 5)$ representa a sequência $\{(0, 1), (1, 2), (2, 2), (3, 5)\}$.

Note que a sequência (2) não é a mesma coisa que o inteiro 2, e a sequência $(2, 3)$ não é a mesma coisa que o par ordenado $(2, 3)$. Devido a esta confusão, alguns autores (e algumas linguagens de programação) usam outros símbolos, no lugar de parênteses, para denotar sequências; como colchetes angulares $\langle \dots \rangle$, ou colchetes comuns $[\dots]$.

Note que há também uma diferença entre a sequência (23) e o conjunto $\{23\}$.

7.2.2 Índice inicial padrão

Em matemática (e em algumas linguagens de programação, como FORTRAN), o índice inicial de uma sequência é geralmente 1 por convenção. Uma vantagem desta escolha é que o n -ésimo elemento de uma sequência x é x_n .

Alguns autores, entretanto, preferem numerar os termos a partir de 0. Note que, neste caso, em uma sequência com n termos os índices variam de 0 a $n - 1$. Além disso, o elemento de índice k (ou seja x_k) é o $k + 1$ -ésimo elemento da sequência. Mesmo assim, a numeração a partir de 0 tem certas vantagens em computação, e é o padrão de várias linguagens de programação modernas, como C, Java e Python.

7.2.3 Comprimento

O *comprimento* de uma sequência finita é o número de termos, geralmente denotado por $|x|$.

Exercício 7.23: Se uma sequência tem índice inicial r e índice final s , qual é o seu comprimento? Se ela tem índice inicial 0 e comprimento n , qual é o índice final? E se ela tem índice inicial 1 e comprimento n ?

Há uma única sequência de comprimento zero, a *sequência vazia*, denotada por $()$, que tem domínio vazio e portanto não tem nenhum termo. (Neste caso os índices inicial e final não são definidos. Note que o intervalo $\{r..s\}$ é vazio para quaisquer r e s com $r > s$.)

7.2.4 Concatenação

Informalmente, a *concatenação* de duas sequências finitas x e y é uma sequência finita que tem todos os termos de x , seguidos de todos os termos de y . Por exemplo, a concatenação de $(10, 20, 30)$ e $(40, 50)$ é $(10, 20, 30, 40, 50)$.

Na literatura esta operação pode ser indicada de muitas maneiras, por exemplo com um ponto $x \cdot y$, com uma barra $x|y$, ou com a mera justaposição xy . Obviamente, o comprimento da concatenação é a soma dos comprimentos das duas sequências.

Para definir precisamente este conceito é preciso estabelecer um índice inicial para a sequência resultante. Por exemplo, se convencionarmos que todas as sequências tem índice inicial zero, a concatenação é a sequência z tal que

$$z_n = \begin{cases} x_n, & \text{se } 0 \leq n < p \\ y_{n-p}, & \text{se } p \leq n < p + q \end{cases} \quad (7.1)$$

onde $p = |x|$ e $q = |y|$.

Exercício 7.24: Adapte a fórmula da concatenação (7.1) para a convenção em que todas as sequências tem índice inicial 1.

Exercício 7.25: Escreva a fórmula geral da concatenação (7.1) para o caso em que os domínios de x e y são $\{r'..s'\}$ e $\{r''..s''\}$, respectivamente, e o índice inicial do resultado é r .

Observe que, se o índice inicial é fixo, a concatenação com a sequência vazia não tem efeito nenhum: $x \cdot () = () \cdot x = x$ para qualquer sequência finita x .

7.2.5 Subsequências e subcadeias

Segundo alguns autores, uma *subsequência* de uma sequência x é simplesmente uma restrição y de x a um subconjunto R de seu domínio. Por exemplo, segundo esta definição, a função $y = \{(3, 30), (5, 20)\}$ seria a subsequência de $x = \{(2, 20), (3, 30), (4, 30), (5, 20)\}$ determinada pelo conjunto $R = \{3, 5\}$.

Uma desvantagem desta definição é que a subsequência nem sempre é uma sequência, pois o novo domínio R nem sempre é um intervalo de inteiros consecutivos. Por esse motivo, alguns autores especificam que os termos da subsequência devem ter seus índices alterados para inteiros consecutivos a partir de um início convencional. Com esta definição, e com índice inicial 0, a função $y = \{(0, 30), (1, 20)\}$ seria a subsequência de $x = \{(0, 20), (1, 30), (2, 30), (3, 20)\}$ determinada pelo conjunto $R = \{1, 3\}$.

Alguns autores usam a palavra *subcadeia* para indicar que o conjunto R é um intervalo de inteiros. Muitas linguagens de programação incluem funções para extrair subcadeias de cadeias dadas.

7.2.6 n -uplas

Para qualquer natural n , definimos uma *n -upla ordenada*, ou simplesmente *n -upla*, como sendo uma sequência finita de comprimento n .

Uma 2-upla, como observado acima, pode ser considerada um par ordenado, e é geralmente chamada por esse nome. Para $n \geq 3$ usam-se os nomes *tripla*, *quádrupla*, *quíntupla*, *sêxtupla*, *séptupla*, *óctupla*, etc.. Não há um nome especial consagrado para 1-uplas.

7.3 Produto cartesiano de n conjuntos

O *produto cartesiano* de n conjuntos A_1, A_2, \dots, A_n , denotado por $A_1 \times A_2 \times \dots \times A_n$, é o conjunto das n -uplas ordenadas (a_1, a_2, \dots, a_n) , com $a_i \in A_i$ para $i = 1, 2, \dots, n$.

Se todos os conjuntos A_1, A_2, \dots, A_n são o mesmo conjunto A , o produto cartesiano $A_1 \times A_2 \times \dots \times A_n$ é denotado por A^n .

7.4 Relações n -árias

7.4.1 Definição

Sejam $A_1, A_2, A_3, \dots, A_n$, conjuntos. Uma *relação n -ária entre* estes conjuntos é um sub-conjunto \mathcal{R} de $A_1 \times A_2 \times A_3 \times \dots \times A_n$. Isto é, um elemento de \mathcal{R} é uma n -upla (a_1, a_2, \dots, a_n) , tal que $a_i \in A_i$ para cada i .

O inteiro n é chamado de *grau* ou *ordem* da relação. O *i -ésimo domínio* da relação é o conjunto $\text{Dom}_i(\mathcal{R})$ de todos os elementos de A_i que ocorrem na posição i das suas n -uplas. Ou seja, um elemento x pertence a $\text{Dom}_i(\mathcal{R})$ se, e somente se, existe uma n -upla (a_1, a_2, \dots, a_n) em \mathcal{R} com $a_i = x$.

Exemplo 7.9: Seja \mathcal{R} a relação em $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ definida pelo conjunto das triplas (a, b, c) tais que $a = b = c$. Observe que a tripla $(2, 2, 2) \in \mathcal{R}$ mas a tripla $(-2, 3, 3) \notin \mathcal{R}$. Os domínios $\text{Dom}_1(\mathcal{R})$, $\text{Dom}_2(\mathcal{R})$ e $\text{Dom}_3(\mathcal{R})$ são o conjunto dos números reais, e o grau é 3.

Exemplo 7.10: Seja \mathcal{R} a relação em $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ definida pelo conjunto das triplas (a, b, c) tais que $a^2 + b^2 = c^2$, $a > 0$, e $b > 0$. Observe que a tripla $(3, 4, 5) \in \mathcal{R}$ mas a tripla $(2, 2, 3) \notin \mathcal{R}$. Pode-se verificar que $\text{Dom}_1(\mathcal{R}) = \text{Dom}_2(\mathcal{R}) = \mathbb{N} \setminus \{1, 2\}$; e que os menores elementos de $\text{Dom}_3(\mathcal{R})$ são $\{5, 10, 13, 17, 20, 25, 26, 29, \dots\}$

Exemplo 7.11: Seja \mathcal{R} a relação em $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ definida pelo conjunto das quádruplas (a, b, q, r) tais que $a = b * q + r$. Observe que a quádrupla $(7, 3, 2, 1)$ está em \mathcal{R} mas a quádrupla $(3, 7, 2, 1)$ não está.

7.4.2 Projeção

Seja \mathcal{R} uma relação n -ária, e sejam i_1, i_2, \dots, i_m inteiros distintos entre 1 e n . A *projeção de \mathcal{R} sobre as componentes i_1, i_2, \dots, i_m* é a relação m -ária \mathcal{S} tal que uma m -upla (b_1, b_2, \dots, b_m) está em \mathcal{S} se e somente se existe uma n -upla (a_1, a_2, \dots, a_n) em \mathcal{R} tal que $b_1 = a_{i_1}, b_2 = a_{i_2}, \dots, b_m = a_{i_m}$.

Exemplo 7.12: Seja $\mathcal{R} \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ a relação ternária formada pelas triplas

$$\{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\}.$$

Eis algumas projeções dessa relação sobre diversas listas de componentes:

- Sobre 2 e 3: $\{(10, 200), (20, 200), (30, 100), (30, 300)\}$
- Sobre 1 e 3: $\{(1, 200), (2, 200), (2, 100), (3, 300)\}$
- Sobre 1 e 2: $\{(1, 10), (1, 20), (2, 20), (2, 30), (3, 30)\}$
- Sobre 2 e 1: $\{(10, 1), (20, 1), (20, 2), (30, 2), (30, 3)\}$
- Sobre 1, 2 e 3: $\{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\} = \mathcal{R}$

Exemplo 7.13: Seja $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ a relação ternária que consiste de todas as triplas (a, b, c) tais que $a^2 + b^2 + c^2 = 1$ — isto é, todos os pontos da superfície da esfera de raio 1 e centro na origem do \mathbb{R}^3 . A projeção de \mathcal{R} sobre as componentes 1 e 3 é o conjunto \mathcal{S} de todos os pares $(a, c) \in \mathbb{R} \times \mathbb{R}$ tais que $(\exists b \in \mathbb{R}) a^2 + b^2 + c^2 = 1$. Pode-se verificar que $\mathcal{S} = \{(a, c) \in \mathbb{R} \times \mathbb{R} : a^2 + c^2 \leq 1\}$, ou seja, o disco de raio 1 e centro na origem do plano \mathbb{R}^2 .

Observe que a ordem dos índices i_1, i_2, \dots, i_m é importante. Observe também que, se $m = n$ e os índices forem $1, 2, \dots, n$, a operação não tem efeito — o resultado é a própria relação \mathcal{R} .

Um caso muito comum é a eliminação de uma determinada componente j mantendo a ordem das demais, como no exemplo 7.13. Nesse caso, $m = n - 1$ e os índices i_1, i_2, \dots, i_m são $1, 2, \dots, j - 1, j + 1, \dots, n$.

7.4.3 Permutação de componentes

Para relações binárias, temos o conceito de relação inversa em que é trocada a ordem das duas componentes de cada par. Sua generalização para relações n -árias é a operação de *permutação de componentes*, que rearranja a ordem das componentes de todas as n -uplas, da mesma maneira.

Mais precisamente, dada uma relação n -ária \mathcal{R} e uma permutação i_1, i_2, \dots, i_n dos inteiros $1, 2, \dots, n$, esta operação produz a relação n -ária \mathcal{S} que consiste de todas as n -uplas $(a_{i_1}, a_{i_2}, \dots, a_{i_n})$ tais que (a_1, a_2, \dots, a_n) está em \mathcal{R} .

Por exemplo, dada a relação ternária $\{(1, 20, 350), (2, 20, 300), (4, 40, 400)\}$, podemos formar a relação ternária $\{(20, 350, 1), (20, 300, 2), (40, 400, 4)\}$ substituindo cada tripla (a_1, a_2, a_3) pela tripla rearranjada (a_2, a_3, a_1) .

Note que esta operação é um caso particular da projeção generalizada com índices i_1, i_2, \dots, i_m , em que $m = n$ e os índices são uma permutação dos inteiros $1, 2, \dots, n$. Note também que cada n -upla de \mathcal{R} corresponde a uma única n -upla de \mathcal{S} , e vice-versa.

7.4.4 Restrição

Seja \mathcal{R} uma relação n -ária, e X_1, X_2, \dots, X_n conjuntos arbitrários. Da mesma forma que para relações binárias, definimos a *restrição de \mathcal{R} a esses conjuntos* como a relação \mathcal{S} das n -uplas (a_1, a_2, \dots, a_n) de \mathcal{R} que tem $a_j \in X_j$, para cada j ; ou seja

$$\mathcal{S} = \mathcal{R} \cap (X_1 \times X_2 \times \dots \times X_n)$$

Exemplo 7.14: Considere a relação

$$\mathcal{R} = \{(1, 10, 200), (1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 100), (3, 30, 300)\}.$$

Observe que esta é uma relação entre os conjuntos $A_1 = \{1, 2, 3\}$, $A_2 = \{10, 20, 30\}$, e $A_3 = \{100, 200, 300\}$.

Sejam $X_1 = \{1, 2, 3, 4\}$, $X_2 = \{20, 30, 40\}$, e $X_3 = \{200, 300\}$. A restrição de \mathcal{R} a X_1 , X_2 e X_3 é

$$\mathcal{S} = \{(1, 20, 200), (2, 20, 200), (2, 30, 100), (3, 30, 300)\}$$

7.4.5 Junção

As tabelas abaixo descrevem duas relações ternárias \mathcal{R} e \mathcal{S} . A relação \mathcal{R} é uma relação que associa empregados, salas, funções, e chefe imediato. A segunda relação associa salas, departamentos, e

ramais de telefone.

\mathcal{R}				\mathcal{S}		
Nome	Função	Chefe	Sala	Sala	Ramal	Setor
José	Secretário	Aníbal	S.102	S.101	8233	Vigilância
José	Secretário	Aníbal	S.102	S.102	8247	Financeiro
José	Digitação	Aníbal	S.103	S.102	8250	Patrimônio
Maria	Digitação	Sônia	S.103	S.103	8288	Vendas
Maria	Secretária	Sônia	S.202	S.103	8289	Vendas
Pedro	Assistente	José	S.102	S.104	8300	Pessoal
Luiz	Despacho	Carlos	S.301	S.301	8380	Compras
Luiz	Motorista	Carlos	S.307	S.303	8350	Contabilidade
				S.307	8380	Transporte

Note que há empregados que trabalham em várias salas, salas com vários empregados, salas com mais de um ramal, ramais que servem mais de uma sala, etc. Cruzando estes dados, podemos obter outras relações entre essas entidades. Por exemplo, casando o número da sala nas duas relações, podemos construir a relação \mathcal{T} abaixo:

\mathcal{T}					
Nome	Função	Chefe	sala	Ramal	Setor
José	Secretário	Aníbal	s.102	8247	Financeiro
José	Secretário	Aníbal	s.102	8250	Patrimônio
José	Digitação	Aníbal	s.103	8288	Vendas
José	Digitação	Aníbal	s.103	8289	Vendas
Maria	Digitação	Sônia	s.103	8288	Vendas
Maria	Digitação	Sônia	s.103	8289	Vendas
Pedro	Assistente	José	s.102	8247	Financeiro
Pedro	Assistente	José	s.102	8250	Patrimônio
Luiz	Despacho	Carlos	s.301	8380	Compras
Luiz	Motorista	Carlos	s.307	8380	Transporte

Note que, por exemplo, a linha “(José, Digitação, Aníbal, 8289, Vendas)” foi incluída na relação \mathcal{T} porque existe a quádrupla “(José, Digitação, Aníbal, S.103)” na relação \mathcal{R} , e a tripla “(S.103, 8288, Vendas)” — com o mesmo número de sala — na relação \mathcal{S} . A construção da tabela acima é um exemplo de *junção* de duas relações n -árias para produzir uma terceira relação.

Mais formalmente, seja \mathcal{R} uma relação m -ária e \mathcal{S} uma relação n -ária. Define-se a *junção* das relações \mathcal{R} e \mathcal{S} como sendo a relação $(m + n - 1)$ -ária \mathcal{T} consistindo de todas as tuplas $(a_1, a_2, \dots, a_{m-1}, c, b_1, b_2, \dots, b_{n-1})$, tais que $(a_1, a_2, \dots, a_{m-1}, c) \in \mathcal{R}$ e $(c, b_1, b_2, \dots, b_{n-1}) \in \mathcal{S}$.

Podemos generalizar ainda mais esta operação casando dois ou mais campos ao mesmo tempo. Seja \mathcal{R} uma relação m -ária, \mathcal{S} uma relação n -ária, e p um inteiro positivo menor que m e n . A *junção em p campos* das relações \mathcal{R} e \mathcal{S} é a relação $(m + n - p)$ -ária \mathcal{T} consistindo de todas as tuplas $(a_1, a_2, \dots, a_{m-p}, c_1, c_2, \dots, c_p, b_1, b_2, \dots, b_{n-p})$, tais que $(a_1, a_2, \dots, a_{m-p}, c_1, c_2, \dots, c_p) \in \mathcal{R}$, e $(c_1, c_2, \dots, c_p, b_1, b_2, \dots, b_{n-p}) \in \mathcal{S}$.

Observe que a junção, tal como definida acima, pode ser combinada com operações de permutação e projeção para casar quaisquer campos de duas relações (e não apenas os últimos campos de \mathcal{R} com os primeiros de \mathcal{S}), e eliminar campos desnecessários no resultado.

Relações n -árias e as operações vistas acima são conceitos fundamentais em bancos de dados, especificamente nos *bancos de dados relacionais*.

Exercício 7.26: Mostre que a composição $S \circ R$ de duas relações binárias R e S pode ser obtida por uma junção seguida de uma projeção.

Capítulo 8

Somatórias e produtórias

8.1 Introdução

Muitas quantidades importantes em matemática são definidas como a soma de uma quantidade variável de parcelas também variáveis, por exemplo a soma $2^1 + 2^2 + \dots + 2^n$, para algum inteiro n . Para estas situações, uma notação muito prática é a *somatória* (também chamada *somatório* ou *notação sigma*), introduzida por Joseph Fourier em 1820. Nesta notação, a soma acima é escrita

$$\sum_{k=1}^n 2^k$$

Em geral, a notação sigma tem a forma

$$\sum_{k=m}^n f(k)$$

onde k é uma variável arbitrária (o *índice* ou a *variável indexadora*), $f(k)$ é uma fórmula qualquer que depende de k (o *termo geral* da somatória), e m, n são inteiros que não dependem de k . Esta notação nos diz para incluirmos na soma precisamente aqueles termos $f(k)$ onde k é um inteiro maior ou igual a m e menor ou igual a n , ou seja $m \leq k \leq n$. Esta soma também pode ser escrita

$$\sum_{\substack{k \\ m \leq k \leq n}} f(k)$$

Costuma-se simplificar esta notação para

$$\sum_{m \leq k \leq n} f(k)$$

quando a variável índice k é óbvia pelo contexto. Observe que se $f(k)$ tem o mesmo valor para dois (ou mais) índices k diferentes entre m e n , esse valor deve ser somado duas (ou mais) vezes. Por exemplo, na somatória $\sum_{k=1}^4 k(5-k)$, as parcelas são 4, 6, 6, 4; portanto a soma é 20.

Uma variante mais geral da notação Σ é

$$\sum_{\substack{k \\ P(k)}} f(k)$$

onde k é a variável índice, e P é algum predicado sobre inteiros. Ela representa a soma de todos os valores $f(k)$ tais que $P(k)$ é verdadeiro. Esta forma é mais comum quando temos restrições mais complicadas sobre os índices, como por exemplo

$$\sum_{\substack{1 \leq k \leq 10 \\ k \text{ ímpar}}} k^2 = 1^2 + 3^2 + 5^2 + 7^2 + 9^2 \quad (8.1)$$

$$\sum_{\substack{p \text{ primo} \\ p \text{ divide } 140}} \frac{1}{p} = \frac{1}{2} + \frac{1}{5} + \frac{1}{7} \quad (8.2)$$

Chamaremos de *domínio* da somatória o conjunto dos índices dos seus termos.

Observe que se o domínio é vazio, o valor da somatória é zero, por definição. Em particular, a somatória $\sum_{k=m}^n f(k)$ é zero sempre que $m > n$.

8.2 Somatórias básicas

Algumas somatórias simples tem fórmulas explícitas. Por exemplo:

$$\sum_{k=1}^n 1 = n \quad (8.3)$$

$$\sum_{k=1}^n k = \frac{n(n+1)}{2} = \binom{n+1}{2} \quad (8.4)$$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6} \quad (8.5)$$

$$\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2} \right)^2 \quad (8.6)$$

$$\sum_{k=0}^{n-1} 2^k = 2^n - 1 \quad (8.7)$$

Estas fórmulas podem ser demonstradas facilmente por indução sobre o valor de n (veja exercício 5.22).

8.3 Manipulação de somatórias

A notação Σ pode ser manipulada de várias maneiras. Em primeiro lugar, observe que a variável índice k pode ser substituída por qualquer outra letra i, j, l, \dots que não tenha significado definido no contexto. Podemos também trocar a variável indexadora k por uma variável relacionada a ela de maneira biunívoca, com o intervalo de variação devidamente ajustado.

Exemplo 8.1: Trocando a variável k pela variável $i = k - 1$, temos

$$\sum_{k=1}^n 2^k = \sum_{i=0}^{n-1} 2^{i+1}$$

Note que para modificar o intervalo da variável i usamos a equação $i = k - 1$, enquanto que para modificar o termo usamos a equação equivalente $k = i + 1$.

Exemplo 8.2: Podemos simplificar a somatória (8.1) trocando a variável k por $2i + 1$, resultando em

$$\sum_{i=0}^{\lfloor (n-1)/2 \rfloor} (2i + 1)^2$$

Note que a equação (8.2) não pode ser simplificada desta maneira, pois não se conhece uma fórmula explícita para os números primos.

Damos a seguir mais algumas regras básicas. Nestas somatórias, o domínio K é um conjunto qualquer de inteiros, e f, g são funções de inteiros para números reais.

- *Distributividade:* Para qualquer número c

$$\sum_{k \in K} c f(k) = c \left(\sum_{k \in K} f(k) \right)$$

Esta propriedade nos permite mover fatores constantes (que não dependem do índice) para dentro ou para fora da somatória.

- *Associatividade:*

$$\sum_{k \in K} (f(k) + g(k)) = \sum_{k \in K} f(k) + \sum_{k \in K} g(k)$$

A associatividade nos permite substituir uma somatória de somas pela soma de somatórias sobre os mesmos índices, ou vice-versa.

- *Decomposição do domínio:* Se $\{K_1, K_2\}$ é uma partição de K , então

$$\sum_{k \in K} f(k) = \left(\sum_{k \in K_1} f(k) \right) + \left(\sum_{k \in K_2} f(k) \right)$$

Esta regra diz que podemos quebrar uma somatória em duas somatórias parciais, desde que cada valor do índice apareça no domínio de uma, e apenas uma, dessas duas partes. Esta regra pode ser generalizada para partições do domínio K em qualquer número de partes.

- *Comutatividade:* Se p é uma permutação qualquer de K ,

$$\sum_{k \in K} f(k) = \sum_{k \in K} f(p(k))$$

A comutatividade nos diz que podemos colocar os termos em qualquer ordem. Uma versão mais geral desta regra é:

- *Troca de domínio:* Se p é uma função bijetora qualquer de K para um conjunto $J \subseteq \mathbb{Z}$,

$$\sum_{k \in K} f(p(k)) = \sum_{j \in J} f(j)$$

Note que troca de variável indexadora, como as dos exemplos 8.1 e 8.2, são casos particulares desta regra.

Exemplo 8.3: Seja x uma sequência qualquer de números reais, e considere a somatória $\sum_{k=1}^n (x_{k+1} - x_k)$. Usando as regras acima, podemos reescrever a somatória como segue:

$$\sum_{k=1}^n (x_{k+1} - x_k) = \sum_{k=1}^n x_{k+1} - \sum_{k=1}^n x_k \quad (8.8)$$

$$= \sum_{i=2}^{n+1} x_i - \sum_{k=1}^n x_k \quad (8.9)$$

$$= \sum_{i=2}^n x_i + x_{n+1} - x_1 - \sum_{k=2}^n x_k \quad (8.10)$$

$$= x_{n+1} - x_1 \quad (8.11)$$

A identidade do exemplo 8.3 é conhecida como *somatória telescópica* porque uma parte de cada parcela “está encaixada em” (isto é, cancela) uma parte da parcela anterior, como ocorre com as peças de uma luneta. Podemos usar esta identidade para provar as fórmulas das somatórias de quadrados e cubos da seção 8.2.

Exercício 8.1:[Soma de PA] Calcule a somatória $\sum_{k=0}^{n-1} (a + rk)$, cujas n parcelas são parte de uma progressão aritmética com termo inicial a e passo r arbitrários.

Exemplo 8.4: Para calcular a somatória $\sum_{k=1}^n k^2$, observamos que $(k+1)^3 = k^3 + 3k^2 + 3k + 1$, portanto $(k+1)^3 - k^3 = 3k^2 + 3k + 1$. Temos então que

$$\sum_{k=1}^n ((k+1)^3 - k^3) = \sum_{k=1}^n (3k^2 + 3k + 1)$$

O lado esquerdo é uma soma telescópica, portanto temos

$$(n+1)^3 - 1 = 3 \sum_{k=1}^n k^2 + 3 \sum_{k=1}^n k + \sum_{k=1}^n 1$$

ou seja

$$\begin{aligned} 3 \sum_{k=1}^n k^2 &= (n+1)^3 - 1 - 3 \sum_{k=1}^n k - \sum_{k=1}^n 1 \\ &= (n+1)^3 - 1 - 3n(n+1)/2 - n \\ &= (2n^3 + 3n^2 + n)/2 \end{aligned}$$

Logo

$$\sum_{k=1}^n k^2 = (n(n+1)(2n+1))/6$$

Exemplo 8.5: Calcular a soma $\sum_{k=1}^n k(k+1)$.

$$\sum_{k=1}^n k(k+1) = \sum_{k=1}^n k^2 + \sum_{k=1}^n k \quad (8.12)$$

$$= (1^2 + 2^2 + 3^2 + \dots + n^2) + (1 + 2 + 3 + \dots + n) \quad (8.13)$$

$$= n(n+1)(2n+1)/6 + n(n+1)/2 \quad (8.14)$$

$$= n(n+1)(n+2)/3 \quad (8.15)$$

Exemplo 8.6: Calcular a somatória $\sum_{k=0}^{n-1} 2^k$. Observe que $2^k = 2^{k+1} - 2^k$.

$$\begin{aligned} \sum_{k=0}^{n-1} 2^k &= \sum_{k=0}^{n-1} (2^{k+1} - 2^k) \\ &= 2^n - 2^0 \\ &= 2^n - 1 \end{aligned}$$

Exercício 8.2: Calcule a somatória $\sum_{k=0}^{n-1} b^k$ para um número real b arbitrário diferente de 1 e 0. Observe que $b^k = (b^{k+1} - b^k)/(b-1)$.

Exercício 8.3:[Soma de PG] Calcule a somatória $\sum_{k=0}^{n-1} ar^k$, cujas n parcelas são parte de uma progressão geométrica com termo inicial a e razão r arbitrários.

Exercício 8.4: Calcule a somatória $\sum_{k=1}^n 1/k(k+1)$

Exemplo 8.7: Calcular a somatória $\sum_{k=1}^n k2^{k-1}$. Observe que $2^{k-1} = 2^k - 2^{k-1}$.

$$\sum_{k=1}^n k2^{k-1} = \sum_{k=1}^n k(2^k - 2^{k-1}) \quad (8.16)$$

$$= \sum_{k=1}^n k2^k - \sum_{k=1}^n k2^{k-1} \quad (8.17)$$

$$= \sum_{k=1}^n k2^k - \sum_{k=0}^{n-1} (k+1)2^k \quad (8.18)$$

$$= \sum_{k=1}^n k2^k - \sum_{k=0}^{n-1} k2^k - \sum_{k=0}^{n-1} 2^k \quad (8.19)$$

$$= n2^n - \sum_{k=0}^{n-1} 2^k \quad (8.20)$$

$$= n2^n - (2^n - 1) \quad (8.21)$$

$$= 2^n(n-1) + 1 \quad (8.22)$$

Exercício 8.5: Prove, por indução em n , que

$$\sum_{k=1}^n \sin k\alpha = \frac{(\sin \frac{n}{2}\alpha)(\sin \frac{n+1}{2}\alpha)}{\sin \frac{1}{2}\alpha}$$

para todo $n \in \mathbb{N}$, e todo ângulo α que não é um múltiplo inteiro de 2π .

Exercício 8.6: Sejam F_0, F_1, F_2, \dots os números de Fibonacci, definidos recursivamente por $F_0 = 0, F_1 = 1$, e $F_{n+2} = F_{n+1} + F_n$ para todo número natural n . Prove por indução que

1. Prove que $(\forall n \in \mathbb{N}) \sum_{i=1}^n F_i = F_{n+2} - 1$
2. Prove que $(\forall n \in \mathbb{N}) \sum_{i=1}^n F_i^2 = F_n F_{n+1}$.

Exercício 8.7: Sejam a e b número reais distintos. Prove que, para todo n em \mathbb{N} , vale a igualdade:

$$\sum_{i=0}^n a^i b^{n-i} = \frac{b^{n+1} - a^{n+1}}{b - a}$$

8.4 Somatórias múltiplas

Os termos de uma somatória podem ser especificados por dois ou mais índices, como no exemplo abaixo:

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j, k) = \begin{array}{l} f(1, 2) + f(1, 3) + f(1, 4) + \\ f(2, 2) + f(2, 3) + f(2, 4) + \\ f(3, 2) + f(3, 3) + f(3, 4) \end{array} \quad (8.23)$$

Este mesmo exemplo pode ser também escrito usando duas vezes a notação Σ , isto é, como uma somatória de somatórias:

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j, k) = \sum_{1 \leq j \leq 3} \sum_{2 \leq k \leq 4} f(j, k) = \begin{array}{l} (f(1, 2) + f(1, 3) + f(1, 4)) + \\ (f(2, 2) + f(2, 3) + f(2, 4)) + \\ (f(3, 2) + f(3, 3) + f(3, 4)) \end{array} \quad (8.24)$$

ou então

$$\sum_{\substack{j,k \\ 1 \leq j \leq 3 \\ 2 \leq k \leq 4}} f(j, k) = \sum_{2 \leq k \leq 4} \sum_{1 \leq j \leq 3} f(j, k) = \begin{array}{l} (f(1, 2) + f(2, 2) + f(3, 2)) + \\ (f(1, 3) + f(2, 3) + f(3, 3)) + \\ (f(1, 4) + f(2, 4) + f(3, 4)) \end{array} \quad (8.25)$$

Podemos entender as fórmulas (8.24) e (8.25) como duas maneiras de somar todos os elementos de uma matriz: coluna por coluna ou linha por linha.

8.4.1 Mudança de ordem de somatórias

As fórmulas (8.24) e (8.25) dizem que podemos trocar a ordem de duas somatórias, quando o domínio de cada variável é independente da outra variável:

$$\sum_{j \in J} \sum_{k \in K} f(j, k) = \sum_{j \in J} \sum_{k \in K} f(j, k) = \sum_{k \in K} \sum_{j \in J} f(j, k).$$

Quando o domínio da soma interna depende da variável índice da somatória externa, a troca exige mais cuidado. Por exemplo,

$$\sum_{j=1}^n \sum_{k=j}^n a_{j,k} = \sum_{1 \leq j \leq k \leq n} a_{j,k} = \sum_{k=1}^n \sum_{j=1}^k a_{j,k}.$$

Para entender esta transformação, veja a figura 8.1. Os pontos representam todos os pares (j, k) considerados na somatória central. As setas sólidas indicam a ordem descrita pela somatória dupla da esquerda (por linhas), e as setas tracejadas indicam a da direita (por colunas).

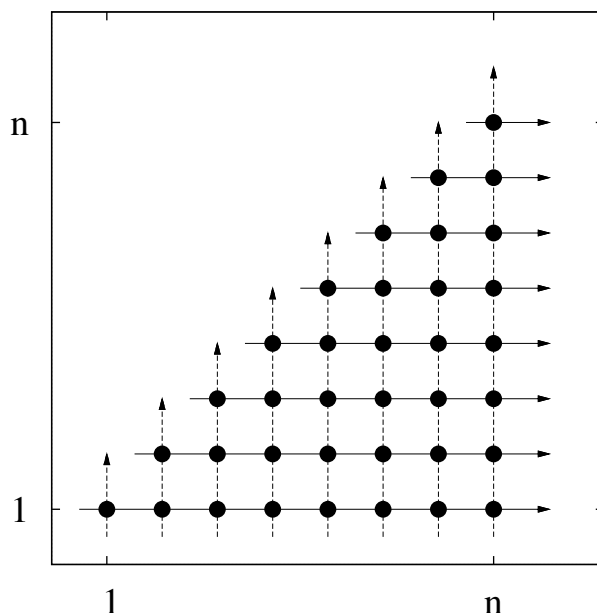


Figura 8.1: Duas maneiras de calcular uma soma dupla. O eixo horizontal é a variável k , o eixo vertical é a variável j .

Exercício 8.8: Para todo número inteiro positivo n , o n -ésimo número harmônico é

$$H_n = \sum_{k=1}^n \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} \dots \frac{1}{n}.$$

Prove que, para todo inteiro n maior ou igual a 2,

$$\sum_{k=1}^{n-1} H_k = nH_n - n.$$

8.4.2 Distributividade generalizada

Outra regra importante para somatórias duplas é a da *distributividade generalizada*, que permite trocar o produto de duas somatórias por uma somatória dupla. Para quaisquer conjuntos $J, K \subseteq \mathbb{Z}$,

e quaisquer funções $f : J \rightarrow \mathbb{R}$, $g : K \rightarrow \mathbb{R}$

$$\left(\sum_{j \in J} f(j) \right) \left(\sum_{k \in K} g(k) \right) = \sum_{\substack{j \in J \\ k \in K}} f(j)g(k) = \sum_{j \in J} \sum_{k \in K} f(j)g(k) \quad (8.26)$$

Note que esta regra também permite trocar uma somatória dupla por um produto de duas somatórias. Para isso basta que o domínio da somatória interna não dependa do índice da soma externa, e que o termo geral possa ser fatorado no produto de duas fórmulas, cada uma delas dependendo de um dos dois índices apenas.

8.5 Majoração de somatórias

Muitas vezes não precisamos saber o valor exato da somatória, basta saber limitante superior ou inferior.

8.5.1 Majoração dos termos

Algumas vezes um bom limitante para o valor de uma somatória pode ser obtido limitando cada um de seus termos pelo termo de maior valor. Por exemplo:

$$\begin{aligned} \sum_{k=1}^n \frac{k+1}{k} &= \frac{2}{1} + \frac{3}{2} + \cdots + \frac{n}{n-1} \\ &\leq \sum_{k=1}^n 2 \\ &= 2n. \end{aligned}$$

Também podemos majorar cada termo da somatória por alguma outra fórmula cuja somatória é conhecida. Por exemplo, observe que, para todo $k \in \mathbb{N}$, temos

$$\frac{k}{k+1} 2^k < 2^k$$

Podemos então concluir que

$$\begin{aligned} \sum_{k=0}^n \frac{k}{k+1} 2^k &< \sum_{k=0}^n 2^k \\ &= 2^{n+1} - 1. \end{aligned}$$

8.5.2 Majoração por indução matemática

No capítulo 5 discutimos a técnica de prova por indução matemática e vimos como usá-la para verificar uma fórmula explícita exata para o resultado de uma somatória. Esta técnica pode ser usada também para provar um limitante superior ou inferior para uma somatória.

Exemplo 8.8: Prove que existe uma constante $c > 0$ tal que

$$\sum_{i=0}^n 3^i \leq c 3^n$$

para todo $n \in \mathbb{N}$.

Embora esta somatória tenha uma fórmula conhecida (soma de progressão geométrica), vamos tentar mostrar a desigualdade sem usar essa fórmula.

Prova:

A tese a ser provada tem a forma $(\exists c > 0)(\forall n \in \mathbb{N}) P(n)$, portanto somente pode ser provada por indução se escolhermos um valor adequado para c . Para isso, podemos escrever um rascunho da demonstração da parte $(\forall n \in \mathbb{N}) P(n)$, por indução em n , deixando o valor de c em aberto; e depois escolher um valor de c que torna todas as partes dessa demonstração válidas.

- *Base:* para $n = 0$, a afirmação $P(n)$ é

$$\sum_{i=0}^0 3^i = 3^0 = 1 \leq c \cdot 1$$

Esta desigualdade será válida se c for maior ou igual a 1.

- *Hipótese de indução:* suponhamos que a desigualdade é verdadeira para algum k , ou seja

$$\sum_{i=0}^k 3^i \leq c3^k$$

- *Passo de indução:* temos de provar que a desigualdade é verdadeira para $k + 1$, isto é temos que mostrar que:

$$\sum_{i=0}^{k+1} 3^i \leq c3^{k+1}$$

Temos que

$$\sum_{i=0}^{k+1} 3^i = \sum_{i=0}^k 3^i + 3^{k+1}$$

Usando a hipótese de indução, temos

$$\begin{aligned} \sum_{i=0}^{k+1} 3^i &\leq c3^k + 3^{k+1} \\ &= \left(\frac{1}{3} + \frac{1}{c}\right)c3^{k+1} \end{aligned}$$

Precisamos agora concluir que

$$\left(\frac{1}{3} + \frac{1}{c}\right)c3^{k+1} \leq c3^{k+1}$$

Isto é verdade se $c \geq 3/2$.

Portanto se escolhermos $c = 3/2$, tanto a base quanto o passo da indução estarão corretos, e a afirmação $(\forall n \in \mathbb{N}) P(n)$ ficará provada.

Fim.

8.5.3 Majoração por integrais

Uma somatória pode ser vista como uma versão discreta de uma integral. Algumas propriedades são de fato comuns aos dois conceitos: por exemplo, se f é um polinômio de grau g , tanto a somatória $\sum_{k=0}^n f(k)$ quanto a integral $\int_0^n f(x) dx$ são polinômios (diferentes) de grau $g + 1$ na variável n . Se f é uma função exponencial, $f(x) = Ar^x$, tanto a somatória quanto a integral são funções exponenciais $ABr^n + C$ (com valores diferentes de B e C). Muitas das regras para manipulação de somatórias (troca de variável, decomposição do domínio, associatividade, etc.) correspondem a regras para manipulação de integrais.

Entretanto, encontrar uma fórmula explícita para uma somatória pode ser mais difícil do que calcular a integral da mesma função. Um exemplo é a somatória $\sum_{k=2}^{n-1} k \log k$, que ocorre na análise da eficiência de algoritmos importantes. A integral correspondente pode ser facilmente calculada (por integração por partes):

$$\int_a^b x \log x dx = \frac{b^2}{2}(\log b - \frac{1}{2}) - \frac{a^2}{2}(\log a - \frac{1}{2})$$

para quaisquer a, b maiores ou iguais a 1. Entretanto, não se conhece uma fórmula explícita simples para a somatória. Porém podemos obter limitantes superior e inferior para a mesma usando a fórmula da integral, como pode ser visto pelo gráfico da figura 8.2.

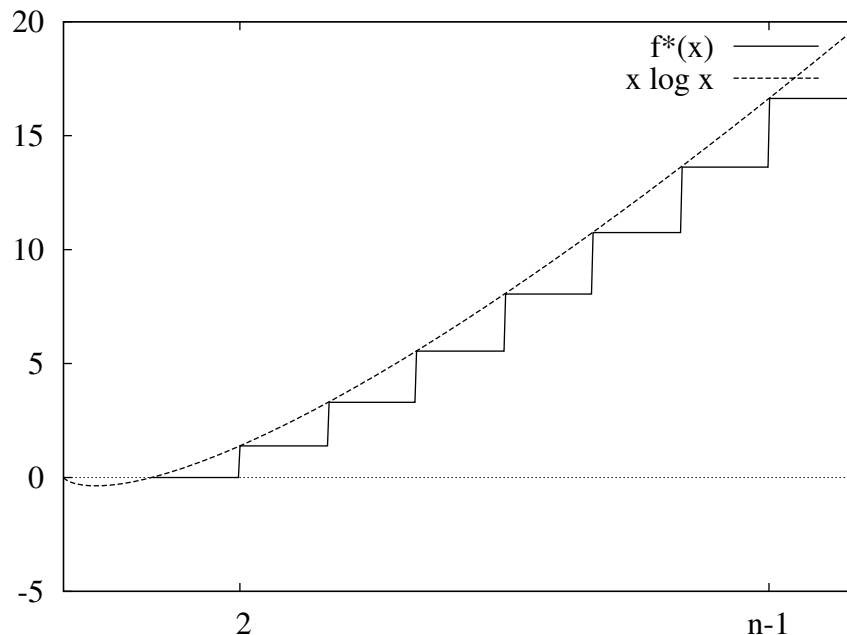


Figura 8.2: Limitante superior por integral.

Nessa figura, a linha em escada é o gráfico da função

$$f^*(x) = [x] \log [x]$$

Observe que, para todo inteiro k , esta função tem valor constante $f^*(x) = k \log k$ para todo x entre

k (inclusive) e $k + 1$ (exclusive). Temos portanto que $\int_k^{k+1} f^*(x) dx = k \log k$, e

$$\int_2^n f^*(x) dx = \sum_{k=2}^{n-1} k \log k$$

Por outro lado, como $\lfloor x \rfloor \leq x$ para todo x , e $x \log x$ é uma função crescente de x , podemos concluir que

$$f^*(x) \leq x \log x$$

para todo x maior ou igual a 2. Veja a figura. Temos portanto que

$$\int_2^n f^*(x) dx \leq \int_2^n x \log x$$

Ou seja

$$\sum_{k=2}^{n-1} k \log k \leq \frac{n^2}{2} \left(\log n - \frac{1}{2} \right) - (2 \log 2 - 1) \quad (8.27)$$

Como $2 \log 2 - 1 > 0$ e $\log n - \frac{1}{2} < \log n$, podemos escrever também que

$$\sum_{k=2}^{n-1} k \log k \leq \frac{n^2}{2} \log n$$

A mesma idéia fornece um limitante inferior para a soma, como ilustrado na figura 8.3.

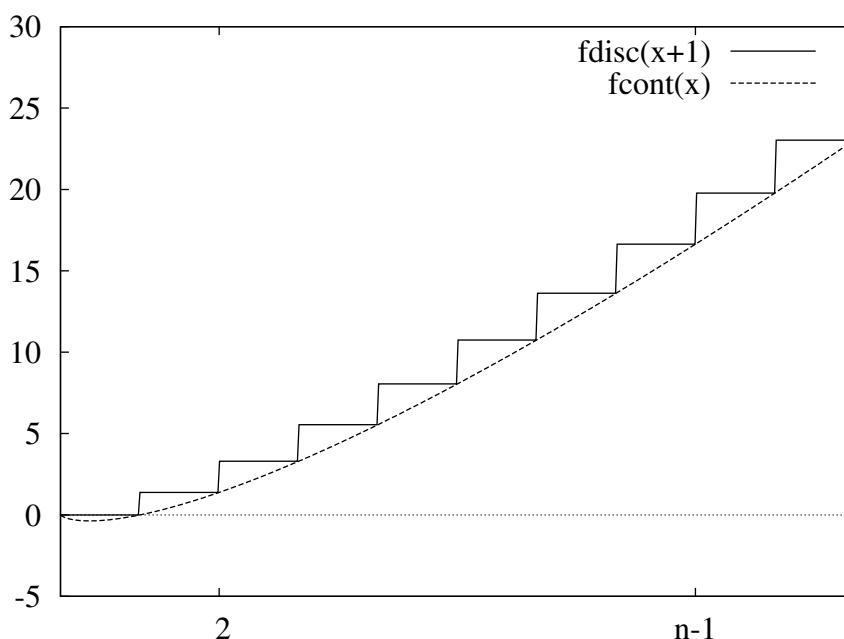


Figura 8.3: Limitante inferior por integral.

Observe que a função f^* deslocada de uma unidade para a esquerda (ou seja, $f^*(x+1)$) está acima do gráfico de $x \log x$ para todo $x \geq 1$, pois $\lfloor x+1 \rfloor > x$ e portanto $\log \lfloor x+1 \rfloor > \log x$. Temos portanto que

$$\int_a^b f^*(x+1) dx \geq \int_a^b x \log(x) dx$$

ou seja

$$\sum_{k=a+1}^{b+1} k \log k \geq \int_a^b x \log(x) dx \quad (8.28)$$

Escolhendo $a = 1$ e $b = n - 1$, obtemos

$$\sum_{k=2}^{n-1} k \log k \geq \int_1^{n-1} u \log u du = \frac{(n-1)^2}{2} (\log(n-1) - \frac{1}{2}) + \frac{1}{4} \quad (8.29)$$

Os limitante (8.27) e (8.29) permitem dizer que, por exemplo

$$20068.3 \leq \sum_{k=2}^{100} k \log k \leq 20525.5$$

Outra maneira de obter um limitante inferior é e observar que

$$\sum_{k=2}^{n-1} k \log k = \sum_{k=2}^n k \log k - n \log n$$

e usar a desigualdade (8.28) para limitar a somatória $\sum_{k=2}^n k \log k$. Tomando $a = 1$ e $b = n$, temos

$$\begin{aligned} \sum_{k=2}^{n-1} k \log k &\geq \int_1^n u \log u du - n \log n = \frac{n^2}{2} (\log n - \frac{1}{2}) + \frac{1}{4} - n \log n \\ &= \frac{n^2}{2} \log n - \frac{n^2}{4} - n \log n + \frac{1}{4} \end{aligned} \quad (8.30)$$

Uma vantagem da fórmula (8.30) é que seu primeiro termo $n^2 \log n$ é igual ao do limitante superior (8.27). Isso permite ver que a diferença entre os dois limitantes (que mede nossa incerteza sobre o valor da somatória) é

$$\Delta = \left(\frac{n^2}{2} \log n - \frac{n^2}{4} - 2 \log 2 + 1 \right) - \left(\frac{n^2}{2} \log n - \frac{n^2}{4} - n \log n + \frac{1}{4} \right) \quad (8.31)$$

$$= n \log n - 2 \log 2 + \frac{3}{4} \quad (8.32)$$

Exercício 8.9: Para todo número inteiro positivo n , o n -ésimo número hamônico é

$$H_n = \sum_{k=1}^n \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} \dots \frac{1}{n}.$$

Prove que $H_n \leq 1 + \ln n$.

Exercício 8.10: Prove que, para todo $n \in \mathbb{N}$,

$$\sum_{k=1}^{n-1} H_{2^k} \geq 1 + \frac{n}{2}.$$

Exercício 8.11: Usando a minoração por integral, prove que $H_n \geq \ln(n+1)$.

Exercício 8.12: Prove que, para todo inteiro positivo n ,

$$\sum_{k=1}^n \frac{1}{2k-1} \leq \frac{1}{2} + \ln \sqrt{n}.$$

Exercício 8.13: Prove que a somatória $\sum_{k=1}^n \frac{1}{k^2}$ tem um limitante superior que não depende de n .

Exercício 8.14: Encontre e prove um limitante superior para $\sum_{k=1}^n k^{5/2}$.

8.6 Somas infinitas

A notação Σ é também usada para *somas infinitas*, também chamadas de *séries*. Uma somatória infinita é o limite de uma somatória finita, quando o valor máximo da variável indexada tende para infinito. Ou seja,

$$\sum_{k=0}^{\infty} f(k) = \lim_{n \rightarrow \infty} \sum_{k=0}^n f(k)$$

Exemplo 8.9: Se x é um número real positivo, então

$$\sum_{k=0}^{\infty} x^k = \lim_{n \rightarrow \infty} \frac{1-x^{n+1}}{1-x} = \begin{cases} 1/(1-x), & \text{se } 0 \leq x < 1 \\ +\infty, & \text{se } x \geq 1 \end{cases}$$

Em particular,

$$\sum_{k=0}^{\infty} \frac{1}{2^k} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 2$$

e

$$\sum_{k=0}^{\infty} 2^k = 1 + 2 + 4 + 8 + \dots = +\infty$$

Observe que o limite pode não existir, ou pode ser infinito. Um exemplo clássico é a soma dos inversos dos inteiros positivos,

$$\sum_{k=1}^{\infty} \frac{1}{k}$$

A soma dos n primeiros termos é o número harmônico H_n ; que é maior ou igual a $\ln(n+1)$ (veja o exercício 8.11), e portanto tende a infinito quando n tende a infinito.

Séries são muito importantes no cálculo diferencial e integral, e são exaustivamente estudadas nessa disciplina. Em computação, somatórias finitas são mais comuns, mas as infinitas também ocorrem ocasionalmente. Por exemplo, se $f(k) \geq 0$ para todo $k \in \mathbb{N}$, temos que

$$\sum_{k=0}^n f(k) \leq \sum_{k=0}^{\infty} f(k)$$

desde que a somatória infinita esteja definida. Esta desigualdade pode oferecer um limitante superior simples para uma somatória finita que não possui uma fórmula fechada simples. Por exemplo,

$$\sum_{k=0}^n \frac{z^k}{k!} \leq \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z$$

Exercício 8.15: Prove que

$$\sum_{k=0}^{\infty} \frac{(k-1)}{2^k} = 0.$$

Exercício 8.16: Encontre um limitante superior para a somatória:

$$\sum_{k=0}^n \frac{k}{3^k}.$$

Exercício 8.17: Obtenha uma fórmula para $\sum_{k=1}^{\infty} kx^k$, supondo que a soma converge. (Dica: calcule a derivada de $\sum_{k=0}^{\infty} x^k$ em relação a x .)

8.7 Produtórias

Sejam m, n números inteiros e f uma função definida sobre os inteiros. A notação

$$\prod_{k=m}^n f(k)$$

denota o produto dos valores $f(k)$ para todos os inteiros k tais que $m \leq k \leq n$.

Uma fórmula deste tipo é chamada de *produtória* ou *produtório*. Se não existe nenhum k no intervalo especificado (isto é, se $m > n$), o valor desta fórmula é 1 (e não zero!), por definição.

Exercício 8.18: Calcule o valor da produtória $\prod_{k=-2}^{+2} k^2 + 1$.

Exercício 8.19: Dê fórmulas explícitas (sem \prod nem ‘...’) para o valor das produtórias abaixo:

- $\prod_{k=1}^n 3$

- $\prod_{k=0}^n 3$

3.
$$\prod_{k=m}^n 3$$

4.
$$\prod_{k=m}^{m+2} 3$$

5.
$$\prod_{k=1}^n k$$

6.
$$\prod_{k=-n}^n k$$

7.
$$\prod_{k=1}^n k^2$$

8.
$$\prod_{k=0}^n 2^k$$

Muitos dos conceitos e técnicas que vimos para somatórias — como troca de índices, separação de termos, mudança de ordem de enumeração, majoração de termos, provas por indução, etc. — podem ser trivialmente adaptadas para produtórias.

Exercício 8.20: Dê fórmulas explícitas (sem \prod nem ‘...’) para o valor das produtórias abaixo:

1.
$$\prod_{k=m}^n k$$

2.
$$\prod_{k=1}^n \frac{k+1}{k}$$

3.
$$\prod_{k=1}^n \prod_{i=1}^m 3^i$$

Uma produtória também pode ser transformada em somatória usando a função logaritmo $\ln x = \log_e x$ e a função exponencial $\exp x = e^x$, onde e é a constante neperiana 2.718281828.... Lembramos que $ab = \exp((\ln a) + (\ln b))$ para quaisquer reais positivos a, b . Podemos então concluir que

$$\prod_{k=m}^n f(k) = \exp\left(\sum_{k=m}^n \ln f(k)\right)$$

Esta identidade pode ser usada, por exemplo para majorar produtórias por integrais.

Exercício 8.21: Determine fórmulas explícitas para as produtórias

- $\prod_{k=1}^n 2 \cdot 4^k$
- $\prod_{k=0}^n \sqrt{k+1}$
- $\prod_{k=2}^n \left(1 - \frac{1}{k^2}\right)$

8.8 Iteração de outras operações

Notações análogas a somatórias e produtórias podem ser usada para indicar a iteração (repetição) de outras operações associativas. Por exemplo, se P é um predicado que depende de um inteiro i , podemos escrever

$$\begin{aligned}\bigvee_{i=1}^n P(i) &= \mathbf{F} \vee P(1) \vee P(2) \vee \cdots \vee P(n) \\ \bigwedge_{i=1}^n P(i) &= \mathbf{V} \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(n) \\ \bigoplus_{i=1}^n P(i) &= \mathbf{F} \oplus P(1) \oplus P(2) \oplus \cdots \oplus P(n)\end{aligned}\tag{8.33}$$

De maneira análoga, se X é uma função que a cada inteiro i associa um conjunto, podemos escrever

$$\begin{aligned}\bigcup_{i=1}^n X(i) &= \emptyset \cup X(1) \cup X(2) \cup \cdots \cup X(n) \\ \bigcap_{i=1}^n X(i) &= \mathcal{U} \cap X(1) \cap X(2) \cap \cdots \cap X(n)\end{aligned}\tag{8.34}$$

Assim como no caso de somatórias, muitas das variações, propriedades e fórmulas de somatórias podem ser adaptadas para estas operações iteradas. Porém, identidades e fórmulas que alteram a ordem dos termos somente valem se a operação for comutativa.

Note que, quando o conjunto de termos é vazio, o resultado é o elemento neutro da operação: \mathbf{F} para \vee e \oplus , \mathbf{V} para \wedge , \emptyset para \cup , e o conjunto universal \mathcal{U} para \cap .

Capítulo 9

Sequências infinitas e recorrências

9.1 Sequências infinitas

Uma *sequência infinita* é uma função cujo domínio é um conjunto de inteiros limitado inferiormente, ou seja $\{n \in \mathbb{Z} : n \geq r\}$ para algum inteiro r ; por exemplo, todos os naturais \mathbb{N} , ou todos os inteiros positivos $\mathbb{N} \setminus \{0\}$. Para estas sequências valem os mesmos conceitos de termo, índice e valor vistos para sequências finitas, bem como a notação x_n em vez de $x(n)$. Além disso, se n é uma variável arbitrária, a fórmula “ x_n ” é chamada de *termo geral* da sequência.

Ocasionalmente o termo sequência também é usado quando o domínio é o conjunto de todos os inteiros \mathbb{Z} ; nesse caso pode-se dizer que a sequência é *bi-infinita*.

Exemplo 9.1: Seja $x : \mathbb{N} \rightarrow \mathbb{R}$ onde $x_n = n^2$, para todo $n \in \mathbb{N}$. Os elementos da sequência são:
 $x_0 = 0, x_1 = 1, x_2 = 4, x_3 = 9, \dots$

Assim como no caso das sequências finitas, a escolha do índice inicial r varia de autor para autor. Em particular, muitos autores definem sequências infinitas como funções dos naturais positivos $\mathbb{N} \setminus \{0\}$. Em outros contextos, entretanto, é conveniente adotar o índice inicial como sendo 0, e definir sequências infinitas como funções com domínio \mathbb{N} (incluindo 0).

O conceito de subsequência também vale para sequências infinitas. Por exemplo, se x é a sequência com domínio \mathbb{N} tal que $x_n = n^2$, e R é o conjunto dos números naturais pares, a subsequência y de x determinada por R seria a restrição de x a R , ou seja, a função

$$y = \{(2k, 4k^2) : k \in \mathbb{N}\} = \{(0, 0), (2, 4), (4, 16), \dots\}$$

Como no caso finito, é conveniente supor que os termos de uma subsequência são re-indexados a partir de um valor convencional (0 ou 1). No exemplo acima, a subsequência de x determinada por R seria a função

$$y = \{(k, 4k^2) : k \in \mathbb{N}\} = \{(0, 0), (1, 4), (2, 16), \dots\}$$

9.2 Especificando sequências infinitas

Uma sequência infinita não pode ser especificada listando todos seus termos. Para definir tal sequência, podemos fornecer uma fórmula para o termo geral x_n que normalmente depende da variável n .

Uma questão comum em matemática discreta e computação é encontrar uma fórmula que representa o termo geral de uma sequência da qual se conhecem apenas alguns termos.

Exemplo 9.2: Seja x uma sequência cujos primeiros termos são x_0, x_1, x_3, \dots são $0, 1, 8, 27, 64, \dots$. Qual é a fórmula para o termo geral x_n ? Pode-se verificar que estes termos satisfazem a fórmula $x_n = n^3$.

Exemplo 9.3: Seja x uma sequência cujos primeiros termos são x_0, x_1, x_3, \dots são $1, 4, 10, 28, 244, 730, \dots$. Qual é a fórmula para o termo geral x_n ? Pode-se verificar que estes termos satisfazem a fórmula $x_n = 3^n + 1$.

Na verdade, este é um problema mal posto, pois sempre existem infinitas fórmulas distintas que fornecem os mesmos resultados para um conjunto finito de valores de n . Por exemplo, outra sequência que também começa com $0, 1, 8, 27, 64, \dots$ é $y_n = n^3 + n(n-1)(n-2)(n-3)(n-4)$. Esta fórmula é diferente de $x_n = n^3$, pois $x_5 = 125$ mas $y_5 = 245$. Em geral, neste tipo de problema o que se deseja é uma fórmula *simples* que seja compatível com os termos dados.

Esta questão faz mais sentido quando existe um algoritmo ou outro critério indireto que define *todos* os valores da sequência. Por exemplo, considere a sequência p cujos termos são os inteiros primos, em ordem crescente de valor. Os primeiros termos dessa sequência são $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots$. Todos os termos da sequência estão bem definidos, e podem ser calculados; porém até hoje não se conhece nenhuma fórmula para o termo geral p_n .

9.3 Recorrência

Muitas sequências importantes são definidas recursivamente, fornecendo-se um ou mais termos iniciais e uma fórmula que determina os demais termos a partir dos termos que os precedem. Essa fórmula é chamada de *recorrência*.

Exemplo 9.4: Uma *progressão aritmética* (PA) é uma sequência x definida pela recorrência

$$\begin{aligned}x_0 &= a \\x_n &= x_{n-1} + r \quad \text{para todo } n > 0\end{aligned}$$

onde a e r são valores reais, chamados de *termo inicial* e *passo* ou *incremento* da progressão.

Pode-se provar facilmente por indução que o termo geral da progressão aritmética do exemplo 9.4 é $x_n = a + nr$, para todo $n \geq 0$; ou seja, uma função linear do índice n .

Exemplo 9.5: Uma *progressão geométrica* (PG) é uma sequência x definida pela recorrência

$$\begin{aligned}x_0 &= a \\x_n &= x_{n-1} \cdot r \quad \text{para todo } n \geq 1\end{aligned}$$

onde a e r são valores reais, chamados de *termo inicial* e *razão* da progressão.

O termo geral de uma progressão geométrica é $x_n = ar^n$, para todo $n \geq 0$; ou seja, uma função exponencial do índice n .

Exemplo 9.6: A sequência dos *números de Fibonacci* é definida por

$$\begin{aligned}f_0 &= 0 \\f_1 &= 1 \\f_n &= f_{n-2} + f_{n-1} \quad \text{para todo } n \geq 2\end{aligned}$$

Os primeiros termos dessa sequência são 0, 1, 1, 2, 3, 5, 8, 13, . . .

Exercício 9.1: No capítulo 5 mostramos que um conjunto de n retas em posição geral divide o plano em $R_n = n(n + 1)/2 + 1$ regiões. Estas regiões também podem ser descritas pela recorrência abaixo:

$$\begin{aligned}R_0 &= 1 \\R_n &= R_{n-1} + n \quad \text{para todo } n \geq 1\end{aligned}$$

Exercício 9.2: Suponha que um casal de tatus começa a dar crias com dois anos de idade, e produz 6 crias (três casais) de tatuzinhos a cada ano. Suponha que um rancho de criação de tatus começou com 1 casal recém-nascido em 2000, e que nenhum tatu foi acrescentado ou eliminado do “rebanho” desde essa época. Escreva uma definição recursiva para o número x_n de tatus que existem no ano n .

9.4 Resolução de recorrências

Determinar uma fórmula explícita para uma sequência definida recursivamente é um problema difícil em geral, mas há técnicas que resolvem certos casos especiais.

9.4.1 Recorrência aditiva simples

Um desses casos especiais são as recorrências da forma $x_n = x_{n-1} + f(n)$ para todo $n \geq m$, onde f é uma função qualquer. A progressão aritmética do exemplo 9.4 é um caso particular desta classe, cuja solução, como vimos, é $x_n = a + rn$. Uma fórmula semelhante resolve recorrências da forma $x_n = x_{n-1} + r$ que valem somente a partir de um índice m diferente de zero.

Exercício 9.3: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_m &= a \\x_n &= x_{n-1} + r \quad \text{para todo } n > m\end{aligned}$$

onde m é uma constante inteira, e a, b são constantes reais que não dependem de n .

No caso da recorrência geral $x_n = x_{n-1} + f(n)$ para todo $n > m$, Pode-se verificar por indução em n que a solução desta recorrência é

$$x_n = x_m + \sum_{k=m+1}^n f(k)$$

Exercício 9.4: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_0 &= 0 \\x_n &= x_{n-1} + n^2 \quad \text{para todo } n > 0\end{aligned}$$

Exercício 9.5: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_1 &= 1 \\x_n &= x_{n-1} + 2^n \text{ para } n > 1\end{aligned}$$

9.4.2 Recorrência multiplicativa simples

Outro caso importante são as recorrências da forma $x_n = f(n)x_{n-1}$ para todo $n > m$, onde f é uma função qualquer. No caso particular da progressão geométrica (exemplo 9.5), em que $f(n)$ é uma constante r , $m = 0$, e $x_0 = a$, a solução, como vimos, é $x_n = ar^n$ para todo $n \geq 0$. Recorrências com índice inicial $m > 0$ tem solução semelhante.

Exercício 9.6: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_m &= a \\x_n &= rx_{n-1} \text{ para todo } n > m\end{aligned}$$

onde m é uma constante inteira, e a, b são constantes reais que não dependem de n .

Quando f é uma função que depende de n , o resultado é uma produtória

$$x_n = x_m \prod_{k=m+1}^n f(k)$$

Exercício 9.7: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_0 &= 1 \\x_n &= \frac{2}{n}x_{n-1} \text{ para todo } n > 0\end{aligned}$$

Exercício 9.8: Determine a fórmula para o termo geral x_n da recorrência

$$\begin{aligned}x_0 &= 1 \\x_n &= \frac{n+p}{n}x_{n-1} \text{ para todo } n > 0\end{aligned}$$

onde p é um número natural que não depende de n .

9.4.3 Recorrências lineares homogêneas

Dizemos que uma relação de recorrência é *linear e homogênea de ordem k* se ela tem a forma

$$x_n = c_1x_{n-1} + c_2x_{n-2} + \cdots + c_kx_{n-k} \quad (9.1)$$

onde k é um inteiro positivo e os coeficientes c_1, c_2, \dots, c_k são números reais, todos independentes de n . Pode-se provar por indução que esta recorrência é satisfeita por uma progressão geométrica $x_n = r^n$, onde r é qualquer raiz do polinômio

$$z^k - c_1z^{k-1} - c_2z^{k-2} - \cdots - c_kz^0 \quad (9.2)$$

Esta fórmula é chamada de *polinômio característico* da recorrência.

Por exemplo, a recorrência $f_n = f_{n-2} + f_{n-1}$ dos números de Fibonacci é linear e homogênea de ordem 2, com coeficientes $c_1 = c_2 = 1$. Ela é satisfeita pelas sequências x e y , onde $x_n = r^n$, $y_n = s^n$, e r, s são as duas raízes da equação $z^2 = z + 1$. Estas raízes são

$$r = \frac{1 + \sqrt{5}}{2} \quad s = \frac{1 - \sqrt{5}}{2} \quad (9.3)$$

A primeira raiz $r = 1.6180339887 \dots$, geralmente denotada pela letra ϕ , é conhecida como *razão áurea*, porque na Grécia antiga os arquitetos e artistas acreditavam que o retângulo com lados 1 e ϕ tinha as proporções mais belas dentre todos os retângulos. A segunda raiz $s = -0.6180339887$, que vários autores denotam por $\hat{\phi}$, é igual a $1 - \phi$ e $-\frac{1}{\phi}$.

n	r^n	s^n
0	1.00000000	1.00000000
1	1.61803399	-0.61803399
2	2.61803399	0.38196601
3	4.23606798	-0.23606798
4	6.85410197	0.14589803
5	11.09016994	-0.09016994
6	17.94427191	0.05572809
7	29.03444185	-0.03444185
\vdots	\vdots	\vdots

Nesta tabela pode-se verificar que $r^2 = r^1 + r^0$, $s^2 = s^1 + s^0$, $r^3 = r^2 + r^1$, e assim por diante.

As sequências x e y são apenas duas das possíveis soluções para a recorrência (9.3). Pode-se provar que qualquer combinação linear destas duas sequências

$$z_n = \alpha x_n + \beta y_n = \alpha \phi^n + \beta \hat{\phi}^n \quad (9.4)$$

também é uma solução da recorrência. Os valores de α e β podem ser obtidos a partir dos valores iniciais dados $f_0 = 0$ e $f_1 = 1$, e são

$$\alpha = 1/\sqrt{5} \quad \beta = -1/\sqrt{5} \quad (9.5)$$

Ou seja

$$f_n = \frac{1}{\sqrt{5}}(\phi^n - \hat{\phi}^n) \quad (9.6)$$

Uma vez que $|\hat{\phi}| = 0.61803399$ é menor que 1, o valor absoluto do termo $\hat{\phi}^n$ da fórmula (9.6) vai diminuindo rapidamente à medida que n aumenta. Portanto,

$$\lim_{n \rightarrow \infty} \frac{f_n}{f_{n-1}} = \phi \quad (9.7)$$

e podemos dizer que

$$f_n \approx \frac{1}{\sqrt{5}}\phi^n \quad (9.8)$$

Esta técnica resolve qualquer recorrência homogênea de ordem k cujo polinômio característico tem k raízes distintas. Quando o polinômio tem raízes iguais, ainda existem k soluções independentes, mas elas tem uma forma um pouco mais complicada. Especificamente para cada raiz r com multiplicidade p , toda sequência $x_n = n^i r^n$, para todo i entre 0 e $p - 1$, é uma solução independente.

Exemplo 9.7: Suponha que um casal de tatus matemáticos começa a dar crias com dois anos de idade, e produz 8 crias (quatro casais) de tatuzinhos a cada ano. Suponha que um rancho de criação de tatus começou com 1 casal recém-nascido em 2000, e que nenhum tatu foi acrescentado ou eliminado do “rebanho” desde essa época. Determine uma fórmula explícita para o número x_n de tatus que existem no ano n .

9.5 Recorrências lineares não homogêneas

Uma *recorrência linear não homogênea* é uma fórmula que define o termo geral x_n como uma combinação linear de termos anteriores, com coeficientes constantes, mais uma função arbitrária do índice n . Por exemplo,

$$\begin{aligned} x_0 &= 0 \\ x_n &= x_{n-1} + 2\frac{n}{n-1}x_{n-1} \text{ para todo } n > 0 \end{aligned} \quad (9.9)$$

Pode-se verificar, por indução, que $x_n = n2^n$ é a solução desta recorrência.

No caso geral, uma recorrência linear não homogênea de ordem k tem a forma

$$\left. \begin{aligned} x_0 &= a_0 \\ x_1 &= a_1 \\ &\vdots \\ x_{k-1} &= a_{k-1} \end{aligned} \right\} \quad (9.10)$$

$$x_n = c_1x_{n-1} + c_2x_{n-2} + \cdots + c_kx_{n-k} + f_n \text{ para todo } n \geq k \quad (9.11)$$

onde $a_0, a_1, \dots, a_{k-1}, c_1, c_2, \dots, c_k$ são constantes (que não dependem de n), e f (o *termo independente*) é uma sequência qualquer. Por exemplo, considere a recorrência

$$\left. \begin{aligned} x_0 &= 2 \\ x_1 &= 2 \end{aligned} \right\} \quad (9.12)$$

$$x_n = x_{n-1} + x_{n-2} + (-1)^n \text{ para todo } n \geq 2 \quad (9.13)$$

Note que esta recorrência é similar à de Fibonacci, exceto pelos termos iniciais e pela parcela ‘+ 1’ na recorrência.

Não há uma técnica geral para resolver recorrências não homogêneas, como (9.10)–(9.11). Entretanto, suponha que conseguimos encontrar *uma* sequência particular x que satisfaz a fórmula do termo geral (9.11), mas não necessariamente os termos iniciais. No exemplo acima, pode-se verificar que $x_n = (-1)^n$ é uma solução para a recorrência (9.13), embora tenha $x_0 = +1$ e $x_1 = -1$. Considere agora a recorrência homogênea similar a (9.13),

$$z_n = z_{n-1} + z_{n-2} \quad (9.14)$$

Como vimos anteriormente, a solução geral para esta recorrência é $z_n = \alpha\phi^n + \beta\hat{\phi}^n$. Verifica-se então que a solução geral para a recorrência original (9.13) é a soma de z_n e da solução particular acima, isto é,

$$z_n = \alpha\phi^n + \beta\hat{\phi}^n + (-1)^n \quad (9.15)$$

Os valores de α e β podem ser então determinados pelas condições iniciais $x_0 = 2$ e $x_1 = 2$, resultando em

$$\begin{aligned}\alpha &= \frac{\phi+2}{2\phi-1} \\ \beta &= \frac{\phi-3}{2\phi-1}\end{aligned}\tag{9.16}$$

e portanto

$$x_n = \frac{\phi+2}{2\phi-1}\phi^n + \frac{\phi-3}{2\phi-1}\hat{\phi}^n + (-1)^n\tag{9.17}$$

De modo geral, podemos resolver a recorrência linear não homogênea (9.10)– (9.11) somando uma solução particular x da equação (9.11) com a solução geral da equação homogênea

$$y_n = c_1y_{n-1} + c_2y_{n-2} + \cdots + c_ky_{n-k} \text{ para todo } n \geq k\tag{9.18}$$

Esta solução geral vai depender de k parâmetros $\alpha_1, \dots, \alpha_k$, que podem ser determinados pelas condições iniciais (9.10).

9.6 Majoração e minoração de recorrências

Muitas vezes é difícil ou impossível obter uma fórmula explícita exata para uma sequência y definida recursivamente sobre um conjunto de índices D . Porém, nesses casos pode ser possível obter um *limitante inferior* para y : uma sequência x , com mesmo domínio D , tal que $x_n \leq y_n$ para todo n em D . Analogamente, pode ser possível obter um *limitante superior*, uma sequência z tal que $y_n \leq z_n$ para todo n em D . Tais limitantes podem ser suficientes para muitos fins — como, por exemplo, reserva de espaço de memória para certa tarefa, ou estimativa do tempo de execução de um programa.

Por exemplo, considere a sequência y tal que

$$\begin{aligned}y_0 &= 3 \\ y_n &= y_{n-1} + \lfloor y_{n-1}/3 \rfloor \text{ para todo } n > 0\end{aligned}\tag{9.19}$$

Os primeiros termos desta sequência são

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
y_n	3	4	5	6	8	10	13	17	22	29	38	50	66	88

Podemos obter um limitante superior para y trocando o lado direito da recorrência por uma fórmula mais simples que seja maior igual a esse termo. Por exemplo,

$$\begin{aligned}z_0 &= 3 \\ z_n &= z_{n-1} + z_{n-1}/3 \text{ para todo } n > 0\end{aligned}\tag{9.20}$$

Podemos provar que $z_n \geq y_n$ para todo $n \in \mathbb{N}$, por indução em n . Basta observar que $z_{n-1} \geq y_{n-1}$, pela hipótese de indução, e que $u \geq \lfloor u \rfloor$ para qualquer número real u . A recorrência de z pode ser simplificada para $z_n = (4/3)z_{n-1}$. Esta é uma progressão geométrica com termo inicial 3 e razão $4/3$, e portanto a solução exata é $z_n = 3(4/3)^n$. Podemos então concluir que $y_n \leq 3(4/3)^n$ para todo n em \mathbb{N} .

De maneira análoga, podemos obter um limitante inferior x observando que $[u] \geq u - 1$ para todo número real u . Obtemos então a recorrência

$$\begin{aligned}x_0 &= 3 \\x_n &= x_{n-1} + (x_{n-1}/3 - 1) \text{ para todo } n > 0\end{aligned}\tag{9.21}$$

Esta recorrência pode ser reescrita $x_n = (4/3)x_{n-1} - 1$.

Capítulo 10

Contagem

Um problema comum em matemática, e especialmente em computação, é contar objetos matemáticos (conjuntos, funções, sequências, etc.) com determinadas propriedades. Por exemplo, quantas maneiras diferentes há de escolher 5 cartas de um baralho com 52 cartas? Quantas palavras (com ou sem significado) podem ser formadas com 5 letras distintas? Quantas maneiras há de ordenar um arquivo de n nomes?

Já encontramos alguns problemas desse tipo nos capítulos anteriores. Na seção 2.8, por exemplo, vimos que o número de subconjuntos de um conjunto com n elementos é 2^n . Neste capítulo vamos examinar alguns dos problemas mais comuns deste tipo.

10.1 Permutações

Seja X um conjunto finito de n elementos. Informalmente, uma *permutação de X* é uma lista dos elementos de X em determinada ordem, sem repetições nem omissões. Mais precisamente, podemos definir uma permutação de X como uma função f bijetora do conjunto $\{0, \dots, n-1\} = \{0, 1, \dots, n-1\}$ para o conjunto X . Podemos interpretar o valor de $f(k)$ como o elemento que está na posição k da lista, contando a partir de 0.

Por exemplo, suponha que X é o conjunto das vogais, $X = \{a, e, i, o, u\}$. A função $\{(0, u), (1, e), (2, i), (3, a), (4, o)\}$ é uma permutação de X . Esta função pode ser escrita também como

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ u & e & i & a & o \end{pmatrix}$$

ou como a sequência (u, e, i, a, o), ou simplesmente *ueiao*; ficando sub-entendido que os índices da sequência começam com 0. Duas outras permutações, distintas dessa, são (u, i, e, a, o) e (e, a, o, i, u).

Quantas permutações de X existem? Quando tentamos escrever uma permutação f , elemento a elemento, é fácil ver que temos n escolhas para o elemento $f(0)$ (qualquer elemento de X); $n-1$ escolhas para $f(1)$ (qualquer elemento de X , exceto $f(0)$); $n-2$ para $f(2)$ (qualquer exceto $f(0)$ e $f(1)$); e assim por diante. Para o penúltimo elemento $f(n-2)$ temos apenas 2 possibilidades, e para o último $f(n-1)$ temos apenas uma. Qualquer série de escolhas resulta em uma permutação distinta. Portanto o número de permutações distintas é

$$n \times (n-1) \times (n-2) \times \dots \times 2 \times 1 = n! \tag{10.1}$$

que é o número de funções bijetoras entre dois conjuntos de n elementos (veja exercício 7.10). Assim, por exemplo, o número de permutações das cinco vogais é $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$.

Observe que se o conjunto X é vazio (isto é, se $n = 0$), há apenas uma permutação possível, que é a sequência vazia () (ou seja, o conjunto vazio de pares índice-elemento). Essa observação justifica a definição de $0!$ como sendo 1.

O fatorial de n cresce muito rapidamente quando n aumenta. Por exemplo, $20! = 2.432.902.008.176.640.000$ — mais de dois quintilhões (bilhões de bilhões)! O fatorial de 50 é aproximadamente 3.04×10^{64} , que é muito maior que o número de átomos no sistema solar. Assim, embora possamos facilmente calcular o número de permutações de um baralho de 52 cartas, é impossível gerar todas essas permutações, em qualquer computador concebível atualmente.

Exercício 10.1: Qual é maior, $10!$ ou 5^{10} ?

10.1.1 Fórmula de Stirling

A fórmula (10.1) não é adequada para calcular $n!$ quando n é muito grande. Por exemplo, para calcular $1000000!$ temos que multiplicar 1000000 de números, e o produto vai crescendo a cada passo; o resultado tem mais de 5 milhões de algarismos. Uma fórmula que permite estimar o valor aproximado do fatorial com menos trabalho foi encontrada por Abraham de Moivre (1667–1754) e James Stirling (1692–1770):

$$\ln n! \approx n \ln n - n + \frac{1}{2} \ln(2\pi n)$$

onde \ln é o logaritmo natural (na base $e = 2.7182818\dots$). Aplicando $\exp(x) = e^x$ em ambos os lados temos

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

10.2 Arranjos

Dado um conjunto finito X de n elementos, e um inteiro $r \in \mathbb{N}$, definimos um *arranjo de r elementos de X* como uma sequência de elementos de X com comprimento r , em determinada ordem e sem repetições. Ou seja, uma função dos inteiros $\{0..r-1\}$ para o conjunto X .

Por exemplo, os arranjos de 3 elementos do conjunto $X = \{a, e, i, o, u\}$ são

```
aei aie eai eia iae iea
aio aoi iao ioa oai oia
aeu aue eau eua uae uea
aiu aui iau iua uai uia
aou auo oau oua uao uoa
eio eoi ieo ioe oei oie
eiu eui ieu iue uei uie
eou euo oeu oue ueo uoe
iou iuo oiu oui uio uoi
```


onde aie significa a sequência (a, i, e) , ou seja a função

$$\begin{pmatrix} 0 & 1 & 2 \\ a & i & e \end{pmatrix}$$

e assim por diante.

Pelo mesmo raciocínio usado na seção 10.1, concluímos que o número de tais arranjos é

$$n \times (n - 1) \times (n - 2) \times \cdots \times (n - r + 1) \quad (10.2)$$

Em muitos livros este número é denotado por A_n^r (lê-se “arranjos de n , tomados r a r ”). Alguns autores usam a notação n^r (lê-se “ n à potência r caindo”). Este número pode ser calculado a partir de fatoriais, pela fórmula

$$\frac{n!}{(n - r)!} \quad (10.3)$$

Note que os fatores do denominador cancelam uma parte dos fatores do numerador, deixando apenas os fatores da fórmula (10.2). Assim, por exemplo, o número de arranjos de 3 vogais, listados acima, é $5!/(5 - 3)! = 5 \times 4 \times 3 = 60$.

Uma maneira de entender a fórmula (10.3) é considerar todas as $n!$ permutações de n elementos, e imaginar o que ocorre se tomarmos apenas os r primeiros elementos de cada uma, para obter os arranjos. Note que duas permutações que diferem apenas na ordem dos $n - r$ elementos descartados produzem o mesmo arranjo. Há $(n - r)!$ maneiras de ordenar esses elementos descartados, sem mexer nos r primeiros. Portanto, para cada arranjo temos $(n - r)!$ permutações.

10.3 Combinações

Outro problema muito comum é contar o número de subconjuntos de tamanho r de um conjunto X de n elementos. Note que este problema é diferente de contar os arranjos de r elementos de X : em ambos os casos desejamos tomar r elementos de X , sem repetições; mas neste caso a ordem dos elementos em cada subconjunto não interessa.

Estes subconjuntos são também chamados de *combinações* de r elementos de X . Assim, por exemplo, as combinações de 3 vogais são

aei aeo aio aeu aiu
aou eio eiu eou iou

onde aiu significa o sub-conjunto $\{a, i, u\}$, e assim por diante.

O número de tais combinações acima é denotado por C_r^n por alguns autores, porém a notação mais comum é $\binom{n}{r}$, que se lê “combinações de n , tomados r a r ”.

Para contar as combinações, podemos determinar o número de arranjos de r elementos, e contar apenas uma vez todos os arranjos que diferem apenas na ordem dos elementos. Por exemplo, os seis arranjos aio , aoi , iao , ioa , oai e oia correspondem à mesma combinação $\{a, i, o\}$.

Como temos r elementos em cada arranjo, concluímos que cada combinação corresponde a $r!$ arranjos diferentes. Portanto, o número de combinações é

$$\frac{A_n^r}{r!} = \frac{n \times (n - 1) \times \cdots \times (n - r + 1)}{r \times (r - 1) \times \cdots \times 1} \quad (10.4)$$

Esta fórmula pode ser escrita em termos de fatoriais

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} \quad (10.5)$$

Exercício 10.2: Quantas “mãos” diferentes de cinco cartas podem ser obtidas de um baralho de 52 cartas?

Exercício 10.3: Há 2^n seqüências distintas de n bits (algarismos 0 e 1). Quantas dessas seqüências tem exatamente k bits iguais a 1?

10.3.1 Casos especiais

Alguns casos especiais são dignos de nota. Para todo $n \in \mathbb{N}$,

$$\binom{n}{0} = \binom{n}{n} = 1$$

Para todo inteiro n positivo,

$$\binom{n}{1} = \binom{n}{n-1} = n$$

e, para todo inteiro n maior que 1,

$$\binom{n}{2} = \binom{n}{n-2} = \frac{n(n-1)}{2}$$

Além disso, é óbvio que $\binom{n}{r}$ é zero se r é maior que n .

Uma vez que o número de elementos de um conjunto é um número natural, a definição de $\binom{n}{r}$ não faz muito sentido quando n e/ou r são negativos. Porém, a experiência mostra que muitos teoremas e fórmulas ficam mais simples quando definimos $\binom{n}{r} = 0$ quando $n < 0$ ou $r < 0$.

10.3.2 Propriedades

A função $\binom{n}{r}$ tem várias propriedades interessantes. Por exemplo, para todo $n, r \in \mathbb{N}$, temos

$$\binom{n}{r} = \binom{n}{n-r}$$

Para demonstrar esta identidade, considere um conjunto X de n elementos, e observe que para cada conjunto de r elementos existe um único conjunto de $n-r$ elementos que é seu complemento, e vice-versa. Ou seja, a operação de complemento em relação a X é uma bijeção entre o conjunto dos subconjuntos de r elementos e o conjunto dos subconjuntos de $n-r$ elementos.

Outra propriedade importante é a *identidade de Pascal*:

$$\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}$$

Exercício 10.5: Mostre que $\sum_{r=0}^n 2^r \binom{n}{r} = 3^n$.

Exercício 10.6: Mostre que $\sum_{r=0}^n (-1)^r \binom{n}{r} = 0$.

Exercício 10.7: Seja X um conjunto de n elementos. Usando a fórmula 10.6, mostre que o número de subconjuntos de X de tamanho par é igual ao número de sub-conjuntos de tamanho ímpar.

Exercício 10.8: Prove que, para todos os naturais k e n com $n \geq k$, temos $\sum_{k=r}^n \binom{k}{r} = \binom{n+1}{r+1}$.

Exercício 10.9: Uma prova tem 10 questões do tipo verdadeiro/falso. Quantas maneiras há de responder essas questões, sem deixar nenhuma em branco, de modo a acertar exatamente 7 delas? E acertar pelo menos 7 delas?

10.3.4 Fórmula recursiva

A fórmula (10.5) não é muito eficiente quando n e r são números grandes, pois o numerador $n!$ e denominador $(n-r)!$ podem ser muito maiores que o resultado final $\binom{n}{r}$. Isto também pode acontecer com a fórmula $A_r^n/r!$, no lado esquerdo da equação (10.4). Uma maneira mais eficiente é utilizar a recorrência

$$\binom{n}{r} = \begin{cases} \frac{n}{r} \binom{n-1}{r-1} & \text{se } n \geq r > 0, \\ 1 & \text{se } n \geq r = 0, \\ 0 & \text{se } n < r \text{ ou } r < 0. \end{cases}$$

Esta recorrência pode ser demonstrada por indução em r . Para provar o passo da indução, basta observar que o lado direito da equação 10.4 pode ser fatorada como segue

$$\binom{n}{r} = \frac{n}{r} \left(\frac{n-1}{r-1} \frac{n-2}{r-2} \cdots \frac{n-r+1}{1} \right)$$

e que a parte entre parênteses é $\binom{n-1}{r-1}$. Podemos portanto calcular $\binom{n}{r}$ pelo algoritmo

1. Se $n < r$ ou $r < 0$, devolva 0. Senão
2. $C \leftarrow 1$
3. Para k variando de 1 a r , faça
 4. $C \leftarrow (C \times (n - k + 1)) / (r - k)$
5. Devolva C .

Neste algoritmo é importante efetuar a multiplicação por $n - k + 1$ antes de dividir por $r - k$. Isto garante que a divisão será exata.

10.4 Cardinalidade da união de conjuntos

Para quaisquer conjuntos finitos A e B , vale a identidade

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{10.6}$$

Esta identidade é fácil de entender pelo diagrama de Venn: ao contar os elementos de A e de B , estamos contando os elementos de $A \cup B$, mas contando em dobro os elementos de $A \cap B$. Pelo mesmo raciocínio podemos concluir que, para quaisquer conjuntos finitos A , B , e C , vale a identidade

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \quad (10.7)$$

As fórmulas (10.6) e (10.7) podem ser generalizadas para n conjuntos finitos A_1, A_2, \dots, A_n :

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_i |A_i| \\ &= - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &= + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &= \dots \\ &= +(-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned} \quad (10.8)$$

Para simplificar esta fórmula, vamos denotar por C_r^n o conjunto de todas as combinações de r elementos do conjunto $\{1, 2, \dots, n\}$. Podemos escrever então

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{r=1}^n (-1)^{r-1} \left(\sum_{X \in C_r^n} \left| \bigcap_{k \in X} A_k \right| \right) \quad (10.9)$$

Esta fórmula para a cardinalidade da união de conjuntos finitos é conhecida pelo nome de *princípio da inclusão e exclusão*.

Exercício 10.10: Quantos números entre 1 e 1.000.000 são quadrados perfeitos, cubos perfeitos, ou são divisíveis por 5?

Exercício 10.11: Na notação decimal, quantos números entre 100000 e 999999 começam com algarismo par, terminam com algarismo maior que 5, ou possuem todos os algarismos iguais?

Exercício 10.12: Demonstre a fórmula (10.8), por indução em n .

10.5 Combinações múltiplas

O número $\binom{n}{r}$ pode ser definido também como o número de maneiras de colocar n objetos distintos em duas caixas distintas, com r elementos na primeira caixa, e $n-r$ na segunda caixa. (Comparando com a definição usada na seção 10.3, pode-se ver que o conteúdo da primeira caixa corresponde ao

sub-conjunto escolhido do conjunto X , com r elementos, e a segunda caixa ao complemento desse sub-conjunto em relação a X .)

Esta definição alternativa pode ser generalizada para qualquer número positivo t de caixas. Ou seja, podemos perguntar quantas maneiras existem de distribuir n objetos em t caixas distintas, com r_1 elementos na caixa 1, r_2 elementos na caixa 2, e assim port diante. Obviamente isso é possível apenas se $r_1 + r_2 + \dots + r_t = n$. Um raciocínio análogo ao utilizado na seção 10.3 permite concluir que esse número é

$$\binom{n}{r_1, r_2, \dots, r_t} = \frac{n!}{r_1! r_2! \dots r_t!} \quad (10.10)$$

Por exemplo, suponha que temos 10 pessoas para distribuir em três comissões A , B e C , com, respectivamente, 5, 3, e 2 membros. Isso pode ser feito de

$$\binom{10}{5, 3, 2} = \frac{10!}{5! 3! 2!} = 2520 \quad (10.11)$$

maneiras distintas.

Exercício 10.13: Quantas maneiras existem de distribuir 5 cartas para cada um de 4 jogadores, de um baralho de 52 cartas? (Note que, além das 4 mãos distribuídas, há também um monte de 32 cartas não distribuídas.)

Exercício 10.14: Quantas maneiras distintas existem de pintar 20 casas com as cores vermelha, azul, verde e amarela (cada casa de uma só cor), sendo que deve haver o mesmo número de casas de cada cor?

Exercício 10.15: Quanto vale $\binom{n}{r_1, r_2, \dots, r_t}$ se $t = 1$? E se $r_t = 0$? E se $r_1 = r_2 = \dots = r_t = 1$?

O número de distribuições de n elementos em t caixas de tamanhos fixos aparece na fórmula da soma de t variáveis, $x_1 + x_2 + \dots + x_t$, elevada a potência n . Mais precisamente, $\binom{n}{r_1, r_2, \dots, r_t}$ é o coeficiente do termo $x_1^{r_1} x_2^{r_2} \dots x_t^{r_t}$ na expansão da fórmula $(x_1 + x_2 + \dots + x_t)^n$:

$$(x_1 + x_2 + \dots + x_t)^n = \sum_{\substack{r_1, r_2, \dots, r_t \\ r_1 + r_2 + \dots + r_t = n}} \binom{n}{r_1, r_2, \dots, r_t} x_1^{r_1} x_2^{r_2} \dots x_t^{r_t}.$$

Esta igualdade é conhecida como *fórmula de Leibniz*. Por exemplo,

$$\begin{aligned}
 (a + b + c)^4 &= \binom{4}{4,0,0}a^4b^0c^0 + \binom{4}{3,1,0}a^3b^1c^0 + \binom{4}{2,2,0}a^2b^2c^0 + \binom{4}{1,3,0}a^1b^3c^0 + \binom{4}{0,4,0}a^0b^4c^0 + \\
 &\quad \binom{4}{3,0,1}a^3b^0c^1 + \binom{4}{2,1,1}a^2b^1c^1 + \binom{4}{1,2,1}a^1b^2c^1 + \binom{4}{0,3,1}a^0b^3c^1 + \\
 &\quad \binom{4}{2,0,2}a^2b^0c^2 + \binom{4}{1,1,2}a^1b^1c^2 + \binom{4}{0,2,2}a^0b^2c^2 + \\
 &\quad \binom{4}{1,0,3}a^1b^0c^3 + \binom{4}{0,1,3}a^0b^1c^3 + \\
 &\quad \binom{4}{0,0,4}a^0b^0c^4 \\
 &= 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4 + \\
 &\quad 4a^3c + 12a^2bc + 12ab^2c + 4b^3c + \\
 &\quad 6a^2c^2 + 12abc^2 + 6b^2c^2 + \\
 &\quad 4ac^3 + 4bc^3 + \\
 &\quad 1c^4
 \end{aligned}$$

Por esta razão, estes números são também chamados de *coeficientes multinomiais*.

Note que o coeficiente binomial $\binom{n}{r}$ equivale ao coeficiente multinomial $\binom{n}{r, n-r}$.

Os coeficientes multinomiais também contam as maneiras de listar t objetos distintos com número especificado de repetições de cada objeto. Mais precisamente, suponha que queremos formar uma lista de comprimento n com t itens distintos, sendo que o primeiro item aparece r_1 vezes na lista, o segundo item aparece r_2 vezes, e assim por diante. O número de listas desse tipo é justamente $\binom{n}{r_1, r_2, \dots, r_t}$.

Capítulo 11

Cardinalidade de conjuntos

No capítulo 2 definimos informalmente a cardinalidade de conjuntos finitos, mas só agora temos condições de dar uma definição mais precisa de cardinalidade, inclusive para conjuntos infinitos.

Definição 11.1: Sejam A e B dois conjuntos. Se existir uma função bijetora $f : A \rightarrow B$, então dizemos que A e B tem a mesma cardinalidade. Denotaremos este fato por $A \sim B$.

Pode-se provar que \sim é uma relação de equivalência. As classes de equivalência da relação \sim são chamadas de *cardinalidades* ou *números cardinais*. A cardinalidade de um conjunto A é geralmente denotada por $|A|$ ou $\#A$. Portanto temos que $A \sim B$ se e somente se $|A| = |B|$.

11.1 Conjuntos finitos

Para cada número natural n definimos $I_n = \{i \in \mathbb{N} : i < n\}$. Por exemplo, $I_5 = \{0, 1, 2, 3, 4\}$. Um conjunto A é dito *finito* se existe um número natural n tal que $A \sim I_n$. Neste caso, dizemos que n é o número de elementos de A .

É fácil ver que dois conjuntos finitos tem a mesma cardinalidade se e somente se eles tem o mesmo número de elementos. Portanto a cardinalidade de um conjunto finito pode ser identificada com seu número de elementos.

Observe que, de acordo com a definição, o conjunto vazio \emptyset é finito e $|\emptyset| = 0$.

11.2 Conjuntos infinitos

Para certos conjuntos A , não existe uma bijeção de A para I_n , para nenhum $n \in \mathbb{N}$. Exemplos incluem o próprio conjunto \mathbb{N} , bem como \mathbb{Z} , \mathbb{Q} e \mathbb{R} . Dizemos que estes conjuntos são *infinitos*.

Poderíamos supor que, como no caso dos conjuntos finitos, os subconjuntos próprios de um conjunto infinito A tem cardinalidades estritamente menores que $|A|$. Porém, os exemplos abaixo mostram que isso não é verdade:

Exemplo 11.1: Seja $\mathbb{E} \subset \mathbb{N}$ o conjunto dos números naturais pares, $\{2k : k \in \mathbb{N}\}$. Considere a função $f : \mathbb{N} \rightarrow \mathbb{E}$ definida por $f(n) = 2n$. A função f é uma bijeção do conjunto dos naturais no conjunto dos números pares. Portanto $\mathbb{N} \sim \mathbb{E}$ e portanto a cardinalidade de \mathbb{N} é a mesma que \mathbb{E} .

Ou seja, é possível retirar elementos de um conjunto infinito sem alterar sua cardinalidade. Verifica-se que esta é uma propriedade geral de conjuntos infinitos. Inclusive, muitos autores usam esta propriedade como definição, dizendo que um conjunto A é infinito se e somente se ele tem um subconjunto próprio B tal que $A \sim B$.

O exemplo acima foi enunciado pelo matemático alemão David Hilbert (1862–1943) na forma de uma anedota: um hotel com infinitos quartos, todos ocupados, de repente recebe infinitos novos hóspedes, e precisa arrumar quartos para eles.

Dois outros exemplos importantes são os seguintes:

Exemplo 11.2: Considere a função $f : \mathbb{N} \rightarrow \mathbb{Z}$ definida por

$$f(n) = (-1)^n \left\lfloor \frac{n+1}{2} \right\rfloor = \begin{cases} k & \text{se } n \text{ é par, } n = 2k \\ -(k+1) & \text{se } n \text{ é ímpar, } n = 2k+1 \end{cases} \quad (11.1)$$

A tabela abaixo ilustra a função f

n	0	1	2	3	4	5	6	7...
$f(n)$	0	-1	1	-2	2	-3	3	-4...

Esta função é uma bijeção de \mathbb{N} para \mathbb{Z} , e portanto $\mathbb{N} \sim \mathbb{Z}$.

Exemplo 11.3: Considere a função $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ definida pela fórmula

$$f(u, v) = \frac{(u+v)(u+v+1)}{2} + u \quad (11.2)$$

A tabela abaixo ilustra a função f . Ela associa a cada par (u, v) um número natural na sequência, segundo diagonais sucessivas:

		v					
		0	1	2	3	4	...
0	0	1	3	6	10	...	
1	2	4	7	11	...		
u 2	5	8	12	...			
3	9	13	...				
4	14	...					
⋮	⋮						

Verifica-se que esta função é uma bijeção de $\mathbb{N} \times \mathbb{N}$ para \mathbb{N} , e portanto $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Exemplo 11.4: Considere a função $f : [0, 1] \rightarrow [0, 2]$ definida por $f(x) = 2x$. Verifica-se que esta função é uma bijeção do intervalo $[0, 1]$ para o intervalo $[0, 2]$, e portanto concluímos que $[0, 1] \sim [0, 2]$. Por raciocínio análogo, podemos concluir que todos os intervalos fechados $[a, b]$ de números reais tem a mesma cardinalidade.

Em vista desses exemplos, poderíamos ser levados a acreditar que todos os conjuntos infinitos tem a mesma cardinalidade, ou seja, que existe apenas um tipo de “infinito”. Essa conjectura foi derrubada pelo matemático Georg Cantor em 1879, que mostrou que os conjuntos \mathbb{N} e \mathbb{R} tem cardinalidades diferentes.

11.3 Conjuntos enumeráveis e contáveis

Um conjunto é dito *enumerável* se ele tem a mesma cardinalidade dos números naturais. Dizemos que um conjunto é *contável* se ele é finito ou enumerável.

Observe que um conjunto A é enumerável se, e somente se é possível listar os elementos do conjunto como uma sequência $\{a_0, a_1, a_2, \dots\}$, isto é, podemos indexá-los pelos números naturais.

O teorema 11.1 mostra que o intervalo aberto $(0, 1)$ não tem a mesma cardinalidade que os números naturais.

Teorema 11.1: O intervalo aberto $(0, 1) = \{x \in \mathbb{R}, 0 < x < 1\}$ não é contável.

Prova:

O conjunto $(0, 1)$ não é finito, portanto precisamos demonstrar apenas que ele não é enumerável. Seja f uma função qualquer de \mathbb{N} para $(0, 1)$. Para cada número real $f(i)$, considere uma representação decimal infinita seja $a_i = 0, a_{i0}a_{i1}a_{i2} \dots$ do mesmo. Temos então uma lista infinita de sequências infinitas de algarismos

$$\begin{aligned} a_0 &= 0, a_{00}a_{01}a_{02} \dots \\ a_1 &= 0, a_{10}a_{11}a_{12} \dots \\ a_2 &= 0, a_{20}a_{21}a_{22} \dots \\ &\vdots \end{aligned}$$

Observe que alguns números reais tem duas representações distintas deste tipo, uma delas terminando com uma sequência infinita de zeros, e a outra com uma sequência infinita de noves. Por exemplo, o número $1/4$ pode ser escrito como $0,250000 \dots$ ou $0,249999 \dots$. Isto ocorre se, e somente se, o número é um racional da forma $m/10^n$, com m e n inteiros, $m \neq 0$ e $n \geq 0$. Se $f(i)$ é um destes números, escolhemos para a_i qualquer das duas representações, arbitrariamente. Todos os outros números reais tem uma, e apenas uma, representação decimal.

Observe também que as sequências $0,000000 \dots$ e $0,999999 \dots$ representam os números 0 e 1 , respectivamente, e portanto não estão no intervalo aberto $(0, 1)$. Porém, exceto por esses dois casos, toda fração decimal infinita que começa com $0, \dots$ representa algum número real no intervalo $(0, 1)$.

Considere agora a representação decimal infinita $b = 0, b_1b_2b_3 \dots$ onde

$$b_i = \begin{cases} 4 & \text{se } a_{ii} \neq 4 \\ 5 & \text{se } a_{ii} = 4 \end{cases}$$

A fração decimal b não aparece na lista acima, pois ela difere de cada fração a_i na i -ésima posição.

Como b usa apenas algarismos 4 e 5 depois da vírgula, o número real b^* que ela representa não é nem 0 nem 1 , e portanto está no intervalo aberto $(0, 1)$. Uma vez que b não termina nem em infinitos zeros nem em infinitos noves, o número b^* tem apenas essa representação, e portanto ele é diferente do número real $f(i)$, para todo i em \mathbb{N} .

Concluimos que nenhuma função f de \mathbb{N} para $(0, 1)$ pode ser sobrejetora. Logo $(0, 1)$ não é enumerável.

Fim.

A técnica usada nesta demonstração para encontrar o contra exemplo b^* é conhecida como *método da diagonalização* (ou *método da diagonalização de Cantor*). Este método é muito usado em lógica matemática e na teoria da computação.

11.4 Comparação de cardinalidades

Sejam A e C conjuntos. Definimos a relação $A \leq C$ se existe um conjunto B tal que $A \sim B$ e $B \subseteq C$. Em outras palavras, $A \leq C$ se e somente se existe uma função injetora de A para C .

Exemplo 11.5: Seja \mathbb{C} o conjunto dos números primos, e \mathbb{M} o conjunto dos quadrados perfeitos, $\{n^2 : n \in \mathbb{N}\}$. Observe que a função f de \mathbb{C} para \mathbb{M} definida por $f(p) = p^2$ é uma função injetora. Portanto, concluímos que $\mathbb{C} \leq \mathbb{M}$.

Em particular, para quaisquer conjuntos A, B tais que $A \subseteq B$, a função identidade I_A é uma função injetora de A para B ; portanto concluímos que $A \subseteq B$ implica $A \leq B$. Em particular, $A \leq A$ para qualquer conjunto A ; ou seja, \leq é uma relação reflexiva. Prova-se também que, se $A \leq B$ e $B \leq C$, então $A \leq C$; isto é, \leq é transitiva. (Veja exercício 11.6)

Finalmente, prova-se que, se $A \leq B$ e $B \leq A$, então $A \sim B$ (isto é, A e B tem a mesma cardinalidade). Porém, a demonstração deste fato (devida a Cantor, Schröder e Bernstein) foge do escopo deste livro [6]. Outro resultado cuja prova não cabe aqui é que, dados quaisquer dois conjuntos A e B , pelo menos uma das condições $A \leq B$ e $B \leq A$ deve ser verdadeira.

Pode-se verificar também (veja exercício 11.7) que se $A \sim A'$, $B \sim B'$, e $A \leq B$, então $A' \leq B'$. Portanto a relação \leq entre conjuntos depende apenas de suas cardinalidades, e não dos conjuntos em si. Podemos então substituir \leq por uma relação entre cardinalidades. Em vista das propriedades acima, esta é uma relação de ordem total, que denotaremos por \leq . Ou seja, dizemos *a cardinalidade de A é menor ou igual à de C* , e escrevemos $|A| \leq |B|$, se e somente se $A \leq B$.

Se $|A| \leq |B|$, mas $|A| \neq |B|$, dizemos que a cardinalidade de A é estritamente menor que a cardinalidade de B , e denotamos esse fato por $|A| < |B|$.

Para conjuntos finitos, a relação de ordem parcial \leq entre cardinalidades coincide com a relação \leq entre números naturais. É fácil ver também que a cardinalidade de um conjunto finito é sempre maior que a cardinalidade de qualquer subconjunto próprio. (Veja o exercício 11.8.) Ou seja, para qualquer conjunto finito A e qualquer conjunto B , temos $B \subset A \rightarrow |B| < |A|$.

11.4.1 Teorema de Cantor

Cantor mostrou também o seguinte resultado importante:

Teorema 11.2: Para todo conjunto A , $|A| < |\mathbb{P}(A)|$.

Dito de outra forma, todo conjunto — finito ou infinito — tem mais subconjuntos do que elementos. Este resultado é óbvio para conjuntos finitos, pois se $|A| = n$ então $|\mathbb{P}(A)| = 2^n$ (vide seção 2.8), e $2^n > n$ para todo natural n . A contribuição de Cantor foi mostrar que vale também para conjuntos infinitos.

Prova:

Seja A um conjunto e f uma função qualquer de A para $\mathbb{P}(A)$, ou seja, uma função f que a cada elemento $a \in A$ associa um subconjunto $f(a) \subseteq A$. Vamos mostrar que f não pode ser uma bijeção de A para $\mathbb{P}(A)$.

Observe que o elemento a pode pertencer ou não ao subconjunto $f(a)$. Considere agora o seguinte conjunto:

$$X = \{a \in A : a \notin f(a)\}$$

Observe que X é um subconjunto de A , logo $X \in \mathbb{P}(A)$. Porém, para todo $a \in A$, temos $f(a) \neq X$: pois se $a \in f(a)$ então $a \notin X$, e se $a \notin f(a)$ então $a \in X$. Portanto f não é sobrejetora em $\mathbb{P}(A)$.

Concluimos que, para qualquer conjunto A , não existe nenhuma bijeção de A para $\mathbb{P}(A)$; ou seja, estes dois conjuntos não tem a mesma cardinalidade.

Por outro lado, observe que existe uma bijeção de qualquer conjunto A para o conjunto $A' = \{\{a\} : a \in A\}$, que é um subconjunto de $\mathbb{P}(A)$. Isto mostra que $|A| \leq |\mathbb{P}(A)|$. Juntando estes dois resultados, concluimos que $|A| < |\mathbb{P}(A)|$.

Fim.

Em particular, a cardinalidade $\mathbb{P}(\mathbb{N})$ é estritamente maior que a de \mathbb{N} .

Não é difícil encontrar uma bijeção entre o intervalo aberto $(0, 1)$ e o conjunto dos números reais \mathbb{R} . Veja exercício 11.4. Portanto, em vista do teorema 11.1 a cardinalidade de \mathbb{R} é estritamente maior que a cardinalidade de \mathbb{N} .

11.4.2 Cardinalidades de Cantor

Tradicionalmente denota-se por \aleph^0 a cardinalidade $|\mathbb{N}|$ do conjunto \mathbb{N} . Usando o teorema de Cantor, podemos definir uma sequência de cardinalidades infinitas, cada vez maiores:

$$\aleph^1 = |\mathbb{P}(\mathbb{N})| < \aleph^2 = |\mathbb{P}(\mathbb{P}(\mathbb{N}))| < \aleph^3 = |\mathbb{P}(\mathbb{P}(\mathbb{P}(\mathbb{N})))| \quad \dots \quad (11.3)$$

Cantor mostrou que $|\mathbb{P}(\mathbb{N})| = |\mathbb{R}|$, e portanto \aleph^1 é a cardinalidade do conjunto \mathbb{R} .

Cantor conjecturou em 1878 que não é possível definir um conjunto com cardinalidade entre \aleph^0 e \aleph^1 — isto é, estritamente maior que \mathbb{N} mas estritamente menor que \mathbb{R} . Esta conjectura ficou conhecida como a *hipótese do contínuo*, e ficou aberta até 1963, quando Paul Cohen (baseado em um teorema provado por Kurt Gödel em 1939) mostrou que, com os axiomas usuais da teoria dos conjuntos, não é possível demonstrar nem essa afirmação nem sua negação. Ou seja, pode-se supor que tais conjuntos existem, ou que não existem — e, nos dois casos, nunca se chegará a uma contradição.

Exercício 11.1: Mostre que \sim é uma relação de equivalência.

Exercício 11.2: Prove que

- para todo número natural m e n , se $I_n \sim I_m$ então $m = n$.
(Sugestão: use indução em n .)

- se A é finito, então existe exatamente um número natural tal que $I_n \sim A$.

Exercício 11.3: Mostre que o conjunto \mathbb{Q} é enumerável.

Exercício 11.4: Prove que $(0, 1) \sim \mathbb{R}$.

Exercício 11.5: Prove todo conjunto infinito tem um subconjunto enumerável.

Exercício 11.6: Prove que, se $A \leq B$ e $B \leq C$, então $A \leq C$.

Exercício 11.7: Prove que se $A \sim A'$, $B \sim B'$ e $A \leq B$, então $A' \leq B'$.

Exercício 11.8: Prove que para qualquer conjunto finito A e qualquer conjunto B , $A \subseteq B$ então $|B| < |A|$.

Exercício 11.9: Prove que, se A é infinito, então para qualquer $n \in \mathbb{N}$ existe um subconjunto de A com cardinalidade n .

Capítulo 12

Introdução à Teoria de Grafos

12.1 Introdução

Informalmente, um grafo é um modelo matemático para representar uma coleção de objetos (chamados *vértices*) que são ligados aos pares por outra coleção de objetos (chamados *arcos* ou *arestas*). Em ilustrações de grafos, os vértices são geralmente representados por pontos, círculos ou caixas, e as arestas por linhas ligando os vértices. veja a figura 12.1. Em tais diagramas entende-se que as posições dos vértices e a forma das linhas são irrelevantes; o grafo representa apenas a *topologia* dos vértices e arestas, isto é, quem está ligado a quem.

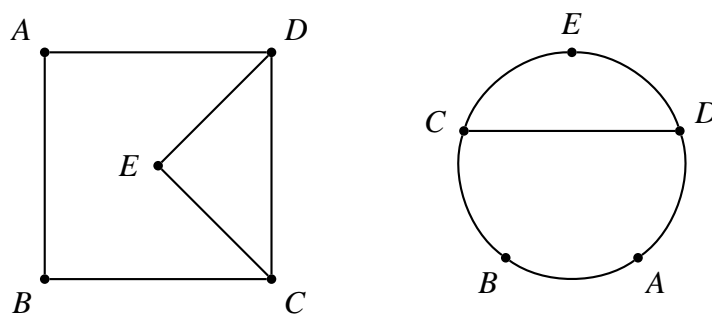


Figura 12.1: Um grafo, desenhado de duas maneiras diferentes.

Grafos são extremamente úteis para modelar problemas em muitas áreas de aplicação. Por exemplo, a malha rodoviária de um estado pode ser representada por um grafo em que as cidades são os vértices, e cada trecho de estrada entre cidades consecutivas é uma aresta. Um circuito elétrico pode ser visto como um grafo onde os vértices são condutores metálicos e as arestas são resistores, capacitores, e outros componentes. Uma molécula pode ser abstraída por um grafo onde os átomos são os vértices e as arestas são as ligações covalentes. Uma treliça metálica pode ser entendida como um grafo onde as arestas são as barras e os vértices são as juntas.

Grafos são especialmente importantes em computação, para modelar tanto hardware em vários níveis (desde circuitos digitais até a internet mundial) quanto conceitos de software (como registros em bancos de dados, blocos e módulos de programas, protocolos de transmissão de dados, e muito mais).

O conceito abstrato de grafo e o estudo matemático de suas propriedades foi uma das muitas contribuições do matemático suíço Leonhard Euler (1707–1783). Um quebra-cabeças famoso na

época era encontrar um passeio que visitasse todas as pontes da cidade de Königsberg (veja a figura 12.2), passando uma única vez em cada ponte. Euler resumiu as propriedades essenciais do mapa por um diagrama de pontos ligados por linhas. Apenas analisando esse diagrama abstrato, ele provou que o tal passeio era impossível. Este trabalho (publicado em 1736) é considerado o primeiro artigo da teoria de grafos.

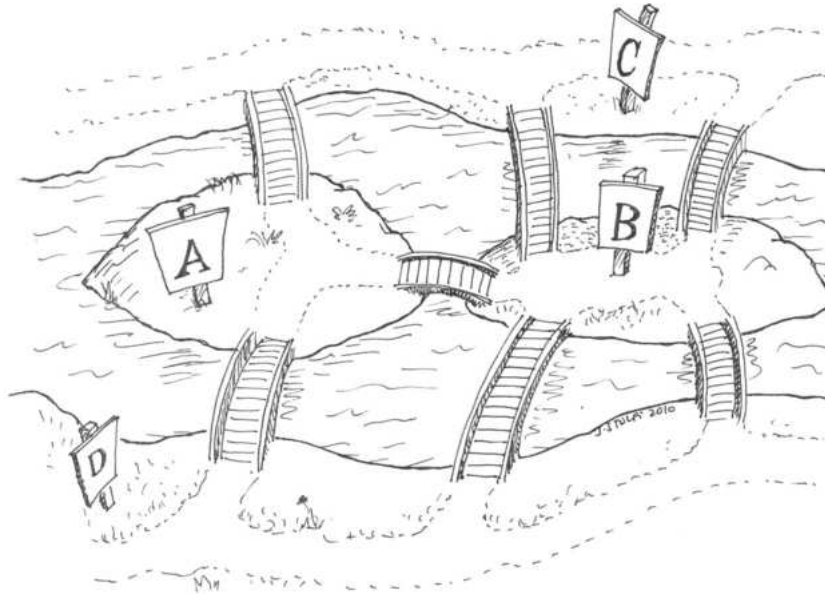


Figura 12.2: O problema das pontes de Königsberg.

A teoria matemática dos grafos foi desenvolvida gradualmente no século 19, quando surgiram importantes aplicações em química e engenharia. Sua importância cresceu muito no século 20, com o surgimento das redes de telefonia, dos circuitos digitais, e por fim dos computadores.

Exercício 12.1: Desenhe o grafo cujos vértices são todos os números inteiros de 2 a 30, sendo que dois vértices estão ligados se e somente se um dos números é divisor do outro.

Exercício 12.2: Escolha uma frase qualquer e desenhe o grafo onde cada vértice representa uma palavra dessa frase, e dois vértices estão ligados entre si se e somente se as duas palavras correspondentes possuem pelo menos uma letra em comum. Assim, por exemplo, gato e cavalo devem ser ligados porque tem as letras a e o em comum; enquanto que gato e peixe não devem ser ligados.

12.2 Variedades de grafos

Há várias maneiras diferentes de formalizar o conceito de grafo em matemática. Cada autor pode adotar uma definição diferente, e qual delas é melhor depende da aplicação. Nesta seção vamos apresentar as definições mais comuns.

Em todas as definições, um grafo G consiste de um conjunto de vértices e um conjunto de arestas, que denotaremos por $\mathcal{V}G$ e $\mathcal{E}G$, respectivamente. O conjunto de vértices é arbitrário; a

natureza das arestas depende da definição, mas cada aresta tem sempre dois *extremos* (não necessariamente distintos) que são vértices de G . Dependendo da definição, um grafo pode ter outras informações além dos conjuntos $\mathcal{V}G$ e $\mathcal{E}G$.

12.2.1 Grafos orientados e não orientados

Um detalhe que varia entre as diferentes definições é a existência de uma *orientação* ou *direção* específica em cada aresta, como a mão única de certas vias urbanas. Grafos que incluem essa informação são ditos *grafos orientados* (ou *dirigidos*), e os que não a registram são *não orientados* (ou *não dirigidos*).

Em um grafo orientado, os extremos de cada aresta são distintos: um vértice é considerado a *origem* da aresta, e o outro seu *destino*. Nas ilustrações de grafos dirigidos, o sentido de cada aresta é geralmente indicado por uma seta da origem para o destino.

12.2.2 Arestas paralelas

Em algumas aplicações, tudo o que precisamos saber sobre as arestas é se dois vértices u e v estão ligados entre si ou não. Nesse caso, o conjunto $\mathcal{E}G$ pode ser definido como um conjunto de pares de vértices: u e v estão ligados se e somente se o par (u, v) está em $\mathcal{E}G$.

Em outras aplicações, pode haver mais de uma ligação entre dois vértices, e esse fato precisa ser levado em conta pelo modelo. Nesses casos, costuma-se definir $\mathcal{E}G$ como outro conjunto arbitrário, independente de $\mathcal{V}G$, e acrescentar ao grafo uma *função de incidência* $\mathcal{F}G$ que, para cada aresta, diz quem são seus dois extremos. Neste modelo, portanto, pode haver um número arbitrário de arestas com os mesmos extremos.

Em um grafo não orientado, duas arestas com os mesmos extremos são ditas *paralelas* (ou *múltiplas*). Em um grafo orientado, duas arestas são paralelas se elas tem os mesmos extremos e a mesma orientação (ou seja, a mesma a origem e mesmo destino). Se elas tem os mesmos extremos mas orientações opostas, elas são ditas *antiparalelas*.

12.2.3 Laços

Uma aresta que liga um vértice a ele mesmo, como uma viela circular que começa e termina na mesma esquina, é chamada de *laço*. Algumas definições permitem laços no grafo; outras proíbem laços, exigindo que os dois extremos de cada aresta sejam vértices distintos.

12.2.4 Grafos simples e multigrafos

Alguns autores definem *grafos simples* como sendo grafos (orientados ou não) sem laços e sem arestas paralelas. Outros definem *grafo* excluindo arestas paralelas, e usam o termo *multigrafo* quando há tais arestas.

12.2.5 Grafos finitos e infinitos

Um grafo pode ter infinitos vértices e/ou infinitas arestas. Tais grafos infinitos tem aplicações na matemática, mas os que ocorrem em computação geralmente são finitos em ambos os aspectos.

No restante deste capítulo vamos considerar apenas grafos finitos.

12.3 Definições formais

Nesta seção veremos como definir formalmente os vários tipos de grafos descritos na seção 12.2.

12.3.1 Arestas como pares ordenados

Alguns autores definem um grafo G como um par $(\mathcal{V}G, \mathcal{E}G)$, onde $\mathcal{V}G$ é um conjunto qualquer, e $\mathcal{E}G$ é uma relação sobre $\mathcal{V}G$, isto é, um subconjunto de $\mathcal{V}G \times \mathcal{V}G$. Nesse caso, cada aresta é um par ordenado de vértices (u, v) . A função de incidência $\mathcal{F}G$ é portanto a função identidade.

De acordo com esta definição, se u e v são vértices distintos de G , os pares (u, v) e (v, u) são arestas distintas. Considera-se portanto que a aresta (u, v) tem uma orientação definida, sendo u a origem e v o destino. O conjunto $\mathcal{E}G$ pode conter apenas a primeira, apenas a segunda, ambas, ou nenhuma. Veja a figura 12.3.

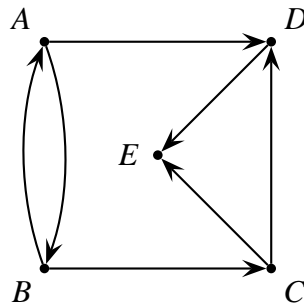


Figura 12.3: Um grafo orientado simples.

Uma consequência importante desta definição é que um grafo não pode ter duas arestas distintas com a mesma origem e o mesmo destino. Ou seja, os grafos definidos desta forma são orientados e não possuem arestas paralelas (mas podem ter arestas antiparalelas).

Neste modelo, um laço é um par (u, u) onde $u \in \mathcal{V}G$. Alguns autores excluem explicitamente laços na definição.

12.3.2 Arestas como pares não ordenados

Outros autores definem uma aresta como sendo um par *não ordenado* de vértices. Segundo estes autores, um grafo G é simplesmente um par de conjuntos $(\mathcal{V}G, \mathcal{E}G)$, onde $\mathcal{V}G$ é arbitrário, e cada elemento de $\mathcal{E}G$ é um conjunto da forma $\{u, v\}$ onde u e v são elementos de $\mathcal{V}G$. Como $\{u, v\}$ e $\{v, u\}$ são o mesmo par não ordenado, neste modelo as arestas não tem direção definida, e não é possível dizer qual dos extremos de uma aresta é a origem e qual é o destino. Veja a figura 12.4.

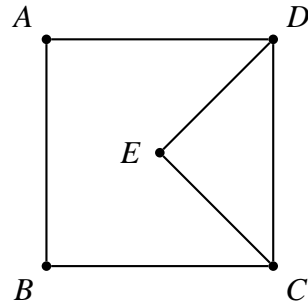


Figura 12.4: Um grafo simples não dirigido.

Uma maneira equivalente de definir o mesmo conceito é dizer que $\mathcal{E}G$ é uma relação *simétrica* sobre $\mathcal{V}G$, ou seja, que o par (u, v) está em $\mathcal{E}G$ se e somente se o par (v, u) também está. Neste caso, os dois pares ordenados (u, v) e (v, u) juntos correspondem ao par não ordenado $\{u, v\}$ da definição anterior.

Uma consequência importante desta definição é que um grafo não pode ter duas arestas distintas com os mesmos extremos. Portanto grafos definidos desta forma não são orientados e não podem ter arestas distintas que sejam paralelas ou antiparalelas.

Note que se u e v são o mesmo vértice, o conjunto $\{u, v\}$ tem apenas um único elemento. Neste modelo, portanto, excluir laços equivale a exigir que toda aresta seja um conjunto com *exatamente* dois elementos, ambos vértices do grafo.

12.3.3 Arestas como objetos com origem e destino

Um grafo G também pode ser definido como uma tripla da forma $(\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$ onde $\mathcal{V}G$ e $\mathcal{E}G$ são conjuntos quaisquer, e $\mathcal{F}G$ é uma função de $\mathcal{E}G$ para $\mathcal{V}G \times \mathcal{V}G$. Ou seja, para cada aresta e existe um único par ordenado de vértices $(u, v) = \mathcal{F}G(e)$ que são os extremos de e ; especificamente, u é a origem de e , e v é o destino.

Observe que este modelo define um grafo orientado e permite arestas paralelas, ou seja podemos ter $e', e'' \in \mathcal{E}G$ com $e' \neq e''$ mas $\mathcal{F}G(e') = \mathcal{F}G(e'')$. Veja a figura 12.5.

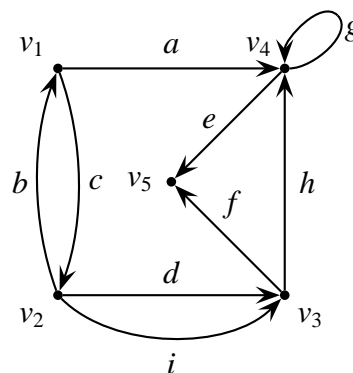


Figura 12.5: Um grafo orientado com arestas paralelas e laços.

Outra maneira equivalente de definir este conceito é dizer que um grafo G é uma quádrupla $(\mathcal{V}G, \mathcal{E}G, \mathcal{F}^-G, \mathcal{F}^+G)$ onde $\mathcal{V}G$ e $\mathcal{E}G$ são conjuntos quaisquer, e tanto \mathcal{F}^-G quanto \mathcal{F}^+G são

funções de $\mathcal{E}G$ para $\mathcal{V}G$, fornecendo respectivamente o vértice de origem e o vértice de destino de cada aresta.

Este modelo também permite laços, ou seja arestas e tais que $\mathcal{F}G(e) = (u, u)$ para algum $u \in \mathcal{V}G$. Alguns autores proíbem laços explicitamente.

12.3.4 Arestas como objetos com dois extremos

Outra opção comum é dizer que um grafo G é uma tripla $(\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$, como na definição anterior, exceto que a função $\mathcal{F}G$ leva cada aresta a um par *não ordenado* de vértices. Isto é, para todo $e \in \mathcal{E}G$, $\mathcal{F}G(e)$ é um conjunto da forma $\{u, v\}$ onde u, v são vértices de G .

Esta definição fornece grafos não orientados com arestas paralelas. Veja a figura 12.6. Assim como a anterior, esta definição também permite laços, que alguns autores excluem explicitamente.

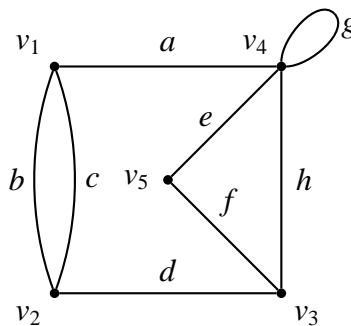


Figura 12.6: Um grafo não orientado com arestas paralelas e laços.

Exercício 12.3: Qual definição de grafo é mais apropriada para o problema das pontes de Königsberg?

Exercício 12.4: Seja V o conjunto dos inteiros entre 2 e 30, inclusive. Qual definição de grafo (orientado ou não, simples ou não, com ou sem laços, etc.) melhor captura cada uma das seguintes informações entre cada par de números de V :

1. Um dos números é maior que o outro.
2. Um dos números é o dobro do outro, menos 2.
3. Um dos números é divisor do outro.
4. Um dos números é divisor próprio do outro.
5. Os dois números possuem um fator primo comum p .
6. Os dois números são relativamente primos entre si.

12.3.5 Convenções para este livro

No restante deste livro adotaremos as definições de *grafo* que permitem arestas paralelas e laços, ou seja as fornecidas nas seções 12.3.3 (para grafos orientados) e 12.3.4 (para grafos não orientados). Quando for conveniente, usaremos o termo *grafo simples* para excluir laços e arestas múltiplas. Nesses casos o conjunto de arestas pode ser modelado por um conjunto de pares, e portanto usaremos as definições das seções 12.3.1 e 12.3.2. Além disso, quando não for especificado o contrário, deve-se entender que os grafos não são orientados.

12.4 Conceitos fundamentais

Há vários conceitos fundamentais que são válidos e importantes para toda a teoria de grafos, qualquer que seja a definição adotada.

12.4.1 Grafo vazio e sem arestas

O conjunto de vértices $\mathcal{V}G$ de um grafo G pode ser vazio. Nesse caso o conjunto de arestas $\mathcal{E}G$ é obrigatoriamente vazio, e a função de incidência também. Portanto existe um único grafo sem vértices, que chamamos de *grafo vazio*.

Por outro lado, se o conjunto de vértices $\mathcal{V}G$ não é vazio, o conjunto de arestas $\mathcal{E}G$ pode ser vazio ou não.

12.4.2 Incidência

Se um vértice v de um grafo G é um dos extremos de alguma aresta e de G , dizemos que e *incide* em v , e vice-versa. Esta propriedade pode ser vista como uma relação entre o conjunto de arestas e o conjunto de vértices, a *relação de incidência* do grafo. (Não confundir com a *função* de incidência, definida na seção 12.2.2, que leva cada aresta ao par dos seus extremos.)

Se o grafo é orientado, podemos dizer, mais especificamente, que uma aresta e com extremos (u, v) *sai* (ou *parte*) do vértice u e *entra* (ou *chega*) no vértice v . Isto define duas relações de $\mathcal{E}G$ para $\mathcal{V}G$, a *relação de saída* e a *relação de chegada*.

12.4.3 Adjacência

Dois vértices u, v são ditos *adjacentes* ou *vizinhos* em um grafo G se e somente se existe uma aresta de G cujos extremos são u e v . Esta relação (simétrica) entre vértices é a *relação de adjacência (não orientada)* do grafo.

Se G é um grafo orientado, pode-se dizer que um vértice u *domina* ou *atinge* outro vértice v se e somente se existe uma aresta de G com origem u e destino v . Esta relação é a *relação de adjacência orientada* ou de *dominância* do grafo G .

Observe que, se as arestas são definidas como pares ordenados de vértices, a relação de adjacência orientada é simplesmente o conjunto $\mathcal{E}G$; e a relação de adjacência não orientada é o fecho simétrico da mesma.

12.4.4 Grau do vértice

Em um grafo G , definimos o *grau* de um vértice v como o número de arestas de G incidentes a v . Nesta definição, cada laço deve ser contado duas vezes. Denotaremos o grau por $d_G(v)$. (Nesta e em outras notações, vamos omitir o subscrito “ G ” quando o grafo estiver determinado no contexto.)

Se o grafo G é orientado, podemos também definir o *grau de entrada* e o *grau de saída* de um vértice v como o número de arestas que entram em v ou saem de v , respectivamente. Denotaremos esses números por $d_G^+(v)$ e $d_G^-(v)$, respectivamente. Note que cada laço é contado uma vez em ambos os graus. Nesse caso, temos que $d_G(v) = d_G^+(v) + d_G^-(v)$.

Teorema 12.1: Em qualquer grafo $G = (\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$, a soma dos graus de todos os vértices é igual ao dobro do número de arestas. Isto é

$$\sum_{v \in \mathcal{V}G} d_G(v) = 2|\mathcal{E}G|$$

Prova:

Cada aresta (laço ou não) contribui duas unidades na soma dos graus.

Fim.

Para grafos orientados, o mesmo argumento permite concluir o seguinte:

Teorema 12.2: Em qualquer grafo orientado $G = (\mathcal{E}V, \mathcal{E}G, \mathcal{F}G)$, a soma dos graus de entrada (ou de saída) de todos os vértices é igual ao número de arestas. Isto é

$$\sum_{v \in \mathcal{V}G} d_G^+(v) = \sum_{v \in \mathcal{V}G} d_G^-(v) = |\mathcal{E}G|$$

Uma consequência do teorema 12.1 é

Corolário 12.3: Em todo grafo $G = (\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$, o número de vértices de grau ímpar é par.

Prova:

Sejam P o conjunto dos vértices de grau par e I o conjunto dos vértices de grau ímpar. Então

$$\sum_{v \in \mathcal{V}G} d_G(v) = \sum_{v \in P} d_G(v) + \sum_{v \in I} d_G(v) = 2|\mathcal{E}G|$$

logo

$$\sum_{v \in I} d_G(v) = 2|\mathcal{E}G| - \sum_{v \in P} d_G(v)$$

O lado direito da equação acima é par. Como a soma de parcelas ímpares é par somente se o número de parcelas for par, concluímos que o $|I|$ é par.

Fim.

Os símbolos Δ_G e δ_G são frequentemente usados para denotar o maior e o menor grau dos vértices, respectivamente, de um grafo G .

12.4.5 Grafos regulares

Um grafo G é *regular* se todos os seus vértices tem o mesmo grau. Em particular se o grau dos vértices é r então G é chamado *r-regular*— regular de grau r . Veja a figura 12.7. Note que um grafo G é r -regular se e somente se $\Delta_G = \delta_G = r$. Se o grafo G é orientado os graus de entrada e saída devem ser iguais.

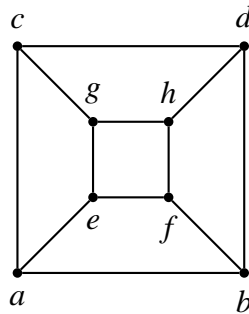


Figura 12.7: O grafo do cubo, um grafo simples 3-regular.

12.4.6 Grafos completos

Um grafo G é chamado *completo* se não tem laços e existe exatamente uma aresta entre cada par de vértices. Note que um grafo completo é sempre um grafo simples e $(n - 1)$ -regular.

Exercício 12.5: Quantas arestas tem um grafo completo com n vértices?

Exercício 12.6: Encontre um limite superior para o número de arestas de um grafo simples.

Exercício 12.7: Quantas arestas possui um grafo k -regular com n vértices?

Exercício 12.8: Desenhe todos os grafos não orientados sem arestas paralelas com vértices $\{1, 2, 3, 4, 5\}$ que são regulares de grau 2.

Exercício 12.9: Desenhe todos os grafos orientados sem arestas paralelas com vértices $\{1, 2, 3, 4\}$ que são regulares de grau 2.

Exercício 12.10: Se G possui vértices v_1, v_2, \dots, v_n , a sequência $(d_{v_1}, d_{v_2}, \dots, d_{v_n})$ é denominada *sequência de graus* de G .

1. Existe um grafo com a seguinte sequência de graus: 3,3,3,3,5,6,6,6,6?
2. Existe um grafo com a seguinte sequência de graus: 1,1,3,3,3,3,5,6,8,9?
3. Existe um grafo *simples* com a sequência de graus do item 2?

12.5 Percursos em grafos

12.5.1 Passeios, trilhas e caminhos

Um *passeio* em um grafo G é uma sequência $P = (v_0, e_1, v_1, \dots, e_k, v_k)$, onde cada v_i é um vértice de G , cada e_i é uma aresta de G , e os extremos de e_i são v_{i-1} e v_i . O inteiro k é o *comprimento*

do passeio, denotado por $|P|$. Quando o grafo é simples podemos definir o passeio apenas pela sequência de seus vértices.

Em particular, um passeio pode ter apenas um vértice e nenhuma aresta, $P = (v_0)$. Tal passeio é dito *trivial*, e seu comprimento é zero.

Dizemos que o passeio P *passa por*, *visita*, ou *atravessa* cada uma das arestas $\{e_1, e_2, \dots, e_k\}$. Dizemos também que P *visita* os vértices $\{v_0, v_1, \dots, v_k\}$, *começa* no vértice v_0 , *termina* no vértice v_k e *passa por* ou *atravessa* cada um dos vértices v_1, v_2, \dots, v_{k-1} . O vértice v_0 é o *início* do passeio, v_k é o *término*, e $\{v_1, v_2, \dots, v_{k-1}\}$ são os *vértices intermediários* ou *internos* do passeio.

Note que a mesma aresta e/ou o mesmo vértice podem ocorrer mais de uma vez; e que o mesmo vértice pode ser ao mesmo tempo início e/ou término e/ou vértice intermediário do passeio. Portanto um passeio de comprimento k visita no máximo $k + 1$ vértices distintos, e tem no máximo $k - 1$ vértices internos.

Se as arestas e_1, e_2, \dots, e_k são todas distintas o passeio é chamado de *trilha*. Note que uma trilha pode repetir vértices.

Um *caminho* em um grafo é um passeio que não repete vértices. É fácil ver que um caminho não pode visitar mais de uma vez a mesma aresta, portanto todo caminho também é uma trilha.

Note que um caminho de comprimento k visita exatamente $k + 1$ vértices distintos e tem exatamente $k - 1$ vértices internos.

Exercício 12.11: Um passeio trivial é uma trilha? É um caminho?

12.5.2 Inversão e concatenação e de passeios

Seja $P = (v_0, e_1, v_1, \dots, e_k, v_k)$ um passeio qualquer em um grafo G . O *passeio inverso*, que denotaremos por P^{-1} , é a sequência dos mesmos vértices e arestas na ordem contrária, isto é $(v_k, e_k, v_{k-1}, e_{k-1}, \dots, v_1, e_1, v_0)$.

Sejam $P = (v_0, e_1, v_1, \dots, e_k, v_k)$ e $Q = (w_0, f_1, w_1, \dots, f_k, w_k)$ dois passeios em um grafo G , tais que o término v_k de P coincide com o início w_0 de Q . Nesse caso definimos a *concatenação* de P com Q como sendo a sequência $(v_0, e_1, v_1, \dots, e_k, v_k, f_1, w_1, \dots, f_k, w_k)$, que denotaremos por $P \cdot Q$. É fácil ver que $P \cdot Q$ também é um passeio em G . Se o término de P não coincide com o início de Q , a concatenação $P \cdot Q$ não é definida.

Exercício 12.12: Qual é a relação entre $|P|$, $|Q|$, e $|P \cdot Q|$?

Exercício 12.13: Se $P \cdot Q$ está definido e é igual a P , o que podemos dizer sobre P e Q ?

Exercício 12.14: Se $P \cdot Q^{-1}$ está definido, o que podemos dizer sobre P e Q ?

Exercício 12.15: Seja G um grafo, e sejam u, v dois vértices quaisquer de G . Prove que existe um **passeio** de u para v em G se e somente se existe um **caminho** de u para v em G .

Exercício 12.16: Prove a seguinte afirmação, ou mostre um contra exemplo: Se P e Q são caminhos em um grafo G , e o término de P é igual ao início de Q , então a concatenação $P \cdot Q$ é um caminho em G .

12.5.3 Circuitos e ciclos

Dizemos que um passeio $P = (v_0, e_1, v_1, \dots, e_k, v_k)$ é *fechado* se $v_0 = v_k$, isto é, se ele começa e termina no mesmo vértice.

Um *circuito* ou *ciclo* em um grafo G é um passeio fechado $(v_0, e_1, v_1, \dots, e_{k-1}, v_{k-1}, e_k, v_k)$ com $k \geq 1$ que não repete vértices nem arestas exceto $v_0 = v_k$.

Um circuito ou ciclo de comprimento k é chamado um k -*ciclo* ou k -*circuito*. Um *grafo ciclo* ou *grafo circuito* é um grafo onde existe um circuito que passa por todos os vértices e todas as arestas. Um grafo sem circuitos é chamado grafo *acíclico*.

Exercício 12.17: Um passeio trivial é um passeio fechado? É um circuito?

Exercício 12.18: Seja P um passeio fechado $(v_0, e_1, v_1, \dots, e_k, v_k)$ com $k \geq 1$ tal que $(v_0, e_1, v_1, \dots, e_{k-1}, v_{k-1})$ constitui um caminho. O passeio P é um circuito?

Exercício 12.19: Seja P um passeio fechado $(v_0, e_1, v_1, \dots, e_k, v_k)$ com $k \geq 1$ que não repete vértices exceto $v_0 = v_k$. O passeio P é um circuito?

Exercício 12.20: Um grafo ciclo é regular?

Exercício 12.21: Prove que um grafo G possui uma trilha fechada se e somente se ele possui um circuito.

Exercício 12.22: Seja G um grafo onde todo vértice tem grau maior ou igual a 2. Prove que G tem um circuito.

12.5.4 Passeios orientados

A definição de passeio da seção 12.5.1 não leva em conta a orientação das arestas, e portanto é geralmente usada em grafos não orientados. Se o grafo G é orientado, podemos definir *passeio orientado* como sendo um passeio $(v_0, e_1, v_1, \dots, e_k, v_k)$ que respeita a orientação de cada aresta; isto é, onde cada aresta e_i tem origem v_{i-1} e término v_i . Os conceitos de trilha, caminho, e circuito orientado são definidos da mesma forma.

Exercício 12.23: Se P é um passeio orientado, o passeio inverso P^{-1} pode ser orientado? E se P for um circuito?

Exercício 12.24: Seja G um grafo orientado, e sejam u, v dois vértices quaisquer de G . Prove que existe um **passeio** orientado de u para v em G se e somente se existe um **caminho** orientado de u para v em G .

12.6 Subgrafos

Um grafo H é um *subgrafo* de outro grafo G se $\mathcal{V}H \subseteq \mathcal{V}G$, $\mathcal{E}H \subseteq \mathcal{E}G$, e cada aresta de $\mathcal{E}H$ tem os mesmos extremos em H e em G . Se G é orientado, H também precisa ser orientado e as arestas precisam ter também a mesma orientação. Ou seja, $\mathcal{F}H$ é a restrição $\mathcal{F}G$ a $\mathcal{E}H$. Veja a figura 12.8. Dado o grafo G , cada subgrafo H é completamente determinado pelos conjuntos $\mathcal{V}H$ e $\mathcal{E}H$. Se $\mathcal{V}H = \mathcal{V}G$ o subgrafo H é chamado *subgrafo gerador* ou *subgrafo espalhado*.

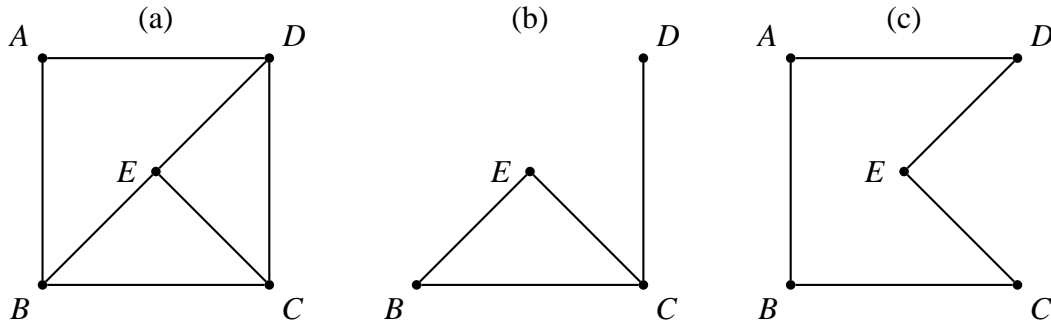


Figura 12.8: (a) Um grafo. (b) Um dos seus subgrafos. (c) Um subgrafo gerador.

Se X é um subconjunto de $\mathcal{V}G$, define-se o *subgrafo de G induzido por X* , denotado por $G[X]$, como sendo o maior subgrafo de G cujo conjunto de vértices é X . Isto é, o subgrafo com esses vértices cujas arestas são todas as arestas de G que possuem ambos os extremos em X . Veja a figura 12.9.

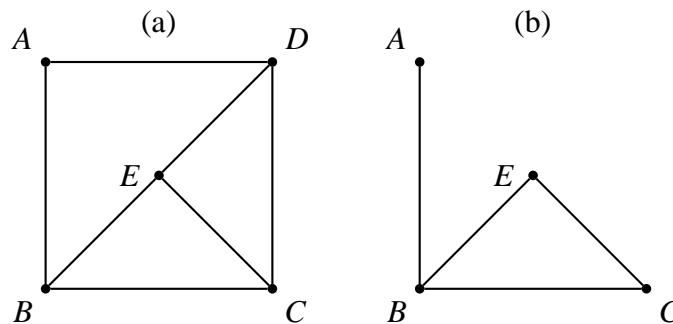


Figura 12.9: (a) Um grafo G . (b) O subgrafo induzido $G[X]$ onde $X = \{A, B, C, E\} \subseteq \mathcal{V}G$.

Analogamente, se Y é um subconjunto de $\mathcal{E}G$, o *subgrafo de G induzido por Y* , também denotado por $G[Y]$, é o menor subgrafo de G cujas arestas são Y . Isto é, o subgrafo que possui apenas essas arestas e os vértices que são extremos delas. Veja a figura 12.10(a).

Finalmente, se $P = (v_0, e_1, v_1, \dots, v_n, e_n)$ é um passeio em um grafo G , definimos o *subgrafo induzido por P* como sendo o subgrafo $G[P]$ cujos vértices são exatamente $\{v_1, v_2, \dots, v_n\}$ e cujas arestas são exatamente $\{e_1, \dots, e_n\}$. Veja a figura 12.10(b).

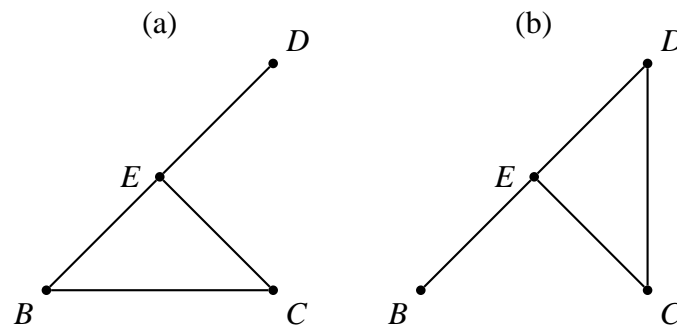


Figura 12.10: (a) O subgrafo induzido $G[Y]$ onde G é o grafo da figura 12.9 e $Y = \{(B, C), (B, E), (C, E), (D, E)\} \subseteq \mathcal{E}G$. (b) O subgrafo induzido $G[P]$ onde P é o passeio (B, E, D, C, E) .

12.6.1 União e intersecção de subgrafos

As operações booleanas de conjuntos de união e intersecção podem ser estendidas para os subgrafos de um grafo. Por exemplo, se H e K são subgrafos de um mesmo grafo G , o *grafo união* $H \cup K$ tem vértices $\mathcal{V}(H \cup K) = \mathcal{V}H \cup \mathcal{V}K$ e arestas $\mathcal{E}(H \cup K) = \mathcal{E}H \cup \mathcal{E}K$; sendo que toda aresta deste grafo tem os mesmos extremos no grafo $H \cup K$ e no grafo G . A intersecção $H \cap K$ de dois subgrafos H e K é definida de maneira análoga. Veja a figura 12.11. Estas definições valem para todos os tipos de grafos definidos na seção 12.3.

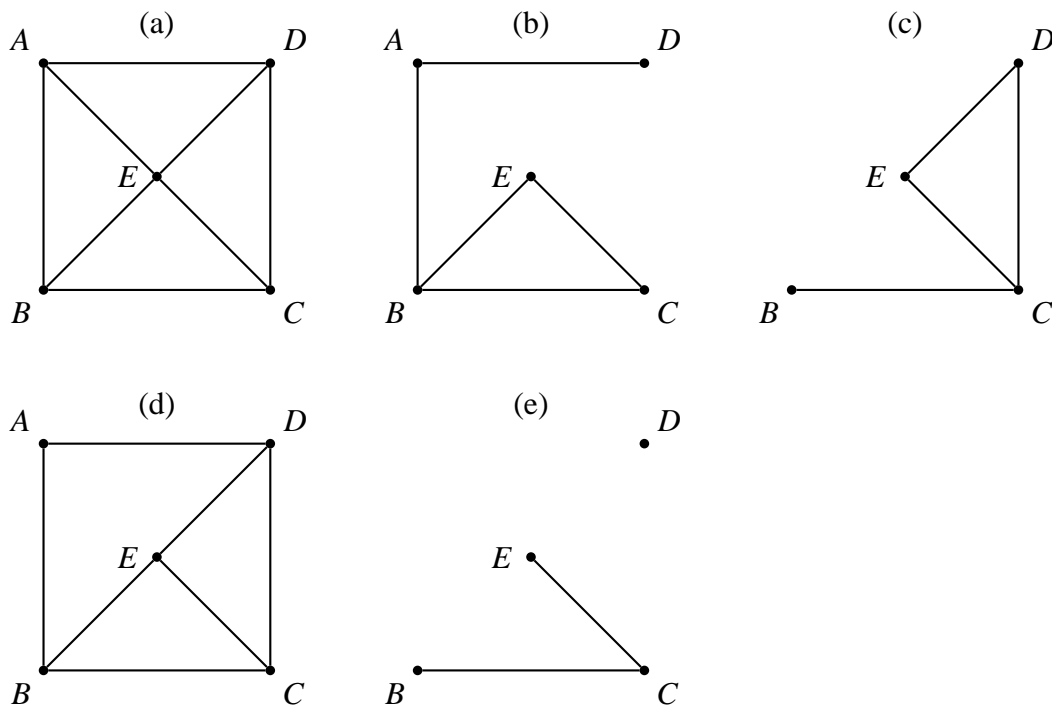


Figura 12.11: (a) Um grafo G . (b) Um dos seus subgrafos H . (c) Um dos seus subgrafos K . (d) O grafo $H \cup K$. (e) O grafo $H \cap K$.

Exercício 12.25: Sejam H e K subgrafos de um grafo G . Prove que $H \cup K$ e $H \cap K$, como definidos acima, são subgrafos de G . Em particular, mostre que, no grafo resultante, os extremos de toda aresta pertencem ao conjunto dos vértices.

Por outro lado, a operação de diferença de conjuntos não tem uma adaptação natural para grafos. Porém, se Y é subconjunto $\mathcal{E}G$, denotamos por $G \setminus Y$ o subgrafo de G que tem vértices $\mathcal{V}G$ e arestas $\mathcal{E}G \setminus Y$. Além disso, se X é um subconjunto de $\mathcal{V}G$, denotamos por $G \setminus X$ o subgrafo $G[\mathcal{V}G \setminus X]$. Note que esta operação retira de G todos os vértices em X e todas as arestas que tem alguma ponta em X .

Exercício 12.26: Seja $Y \subseteq \mathcal{E}G$. Mostre que $G \setminus Y \neq G[\mathcal{V}G \setminus Y]$.

12.6.2 Grafos complementares

Dois grafos simples não orientados G e H são ditos *complementares* se eles tem o mesmo conjunto de vértices V , e para qualquer par de vértices distintos $u, v \in V$, a aresta $\{u, v\}$ está em G se e somente se ela não está em H . No caso de grafos simples orientados, vale a mesma definição, com o par ordenado (u, v) em vez de $\{u, v\}$. Veja a figura 12.12. Dito de outra forma, dois grafos simples G e H são complementares se e somente se $\mathcal{V}G = \mathcal{V}H$, $\mathcal{E}H \cap \mathcal{E}G = \emptyset$, e $\mathcal{E}H \cup \mathcal{E}G$ são todos os pares de vértices distintos. O grafo complementar de um grafo simples G é chamado de *complemento* de G e denotado por \bar{G} . Observe que $G \cup \bar{G}$ é o grafo simples completo com vértices $\mathcal{V}G$.

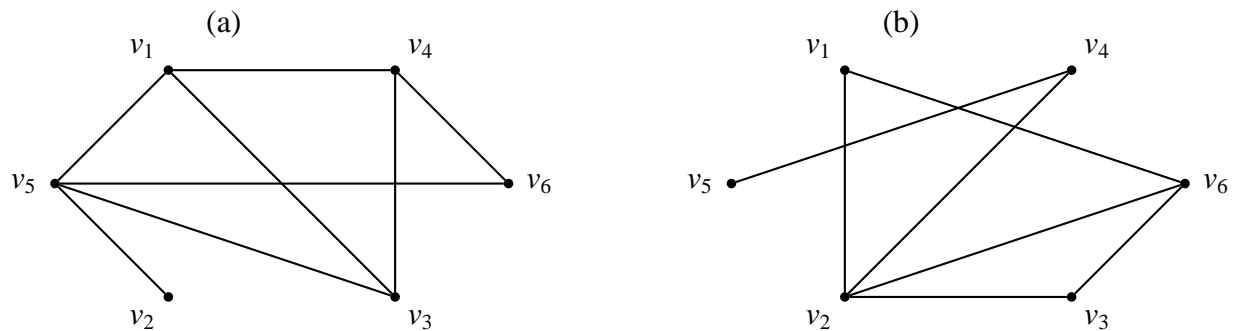


Figura 12.12: (a) Um grafo G . (b) O seu complemento \bar{G}

Exercício 12.27: Formule a seguinte afirmação em termos de grafos, e prove sua validade: “Em qualquer grupo de 6 pessoas, existem três que se conhecem mutuamente, ou três que se desconhecem mutuamente.”

12.7 Representação matricial de grafos

12.7.1 Matriz de adjacência

A *matriz de adjacência* de um grafo finito G é simplesmente a representação matricial da sua relação de adjacência. Ou seja, escolhida uma ordenação total v_0, v_1, \dots, v_{n-1} dos vértices de G , construímos a matriz booleana M de n linhas e n colunas onde $M_{ij} \in \mathbf{V}$ se e somente se $\mathcal{E}G$ inclui

uma aresta com extremos (v_i, v_j) no caso orientado, ou $\{v_i, v_j\}$ no caso não orientado. Observe que, neste segundo caso, a matriz será simétrica ($M_{ij} = M_{ji}$ para quaisquer i e j).

Se as arestas de um grafo são definidas como pares de vértices (ordenados ou não), então o grafo G é completamente determinado pela lista ordenada de vértices v_0, v_1, \dots, v_{n-1} e pela correspondente matriz de adjacência (orientada ou não). Na verdade, dada uma lista ordenada de n vértices, qualquer matriz booleana $n \times n$ determina um grafo orientado com esses vértices; e qualquer matriz simétrica determina um grafo não orientado.

Se a definição permite arestas múltiplas, a matriz booleana de adjacências não é mais suficiente para representar completamente o grafo. Para tal fim, podemos entretanto usar uma matriz M onde cada elemento M_{ij} é um número natural, especificamente o número de arestas com extremos (v_i, v_j) ou $\{v_i, v_j\}$, conforme o caso. Porém, esta representação ainda não permite saber *quais* arestas ligam esses dois vértices.

12.7.2 Matriz de incidência

A *matriz de incidência* de um grafo finito não orientado G é simplesmente a representação matricial da sua relação de incidência. Ou seja, escolhida uma ordenação total v_0, v_1, \dots, v_{n-1} dos vértices de G e uma ordenação total e_0, e_1, \dots, e_{m-1} das arestas, construímos a matriz booleana M de n linhas e m colunas onde M_{ik} é \mathbf{V} se, e somente se o vértice v_i é um extremo da aresta e_k .

Dadas as listas de vértices e arestas, a matriz de incidência determina completamente o grafo, mesmo quando este possui laços ou arestas paralelas.

Exercício 12.28: Seja G um grafo não orientado sem laços, e M sua matriz de incidência, construída a partir de enumerações dadas de seus vértices e arestas. Se considerarmos $\mathbf{V} = 1$ e $\mathbf{F} = 0$, quanto vale a soma dos elementos da linha i de M ? E a soma dos elementos da coluna k ? E a soma de todos os elementos? O que acontece se o grafo tiver laços?

Se G é um grafo orientado, podemos construir duas matrizes de incidência. Na *matriz de entrada* (ou *chegada*) M^+ , o elemento M_{ik}^+ é \mathbf{V} se e somente se a aresta e_k entra no vértice v_i . A *matriz de saída* M^- é definida de maneira análoga.

Em algumas aplicações, é conveniente combinar estas duas matrizes em uma única matriz M cujos elementos são inteiros no conjunto $\{+1, 0, -1\}$; sendo que M_{ik} é $+1$ se e_k entra em v_i , -1 se e_k sai de v_i , e 0 se e_k não incide em v_i . Ou seja, $M_{ik} = M_{ik}^+ - M_{ik}^-$, supondo que $\mathbf{V} = 1$ e $\mathbf{F} = 0$. Entretanto, esta representação somente pode ser usada se o grafo não tiver laços.

12.8 Isomorfismos de grafos

Observe na figura 12.13 os grafos G_1 , G_2 e G_3 tem a mesma estrutura, diferindo apenas nos “nomes” dos vértices e das arestas, e na maneira como estão desenhados; enquanto que o grafo G_4 tem uma estrutura diferente. (Por exemplo, G_4 é o único que tem um circuito de comprimento 4.)

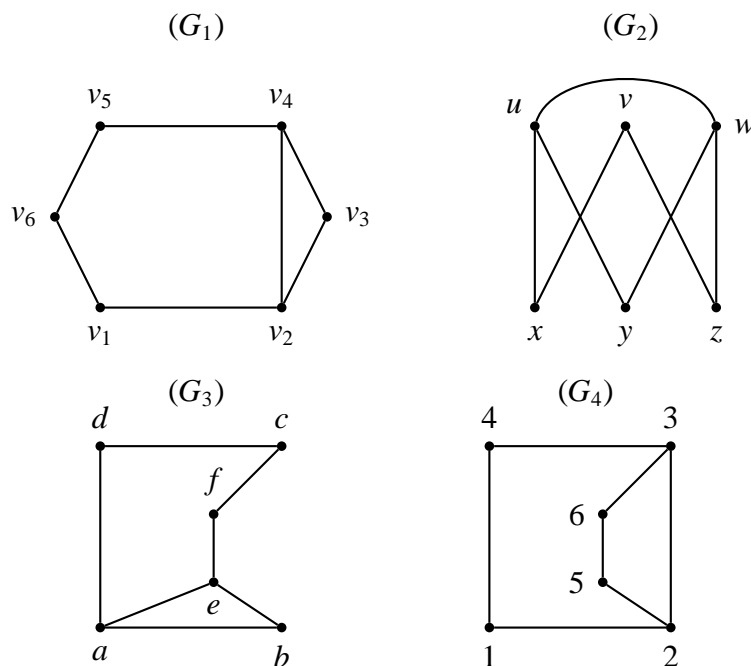
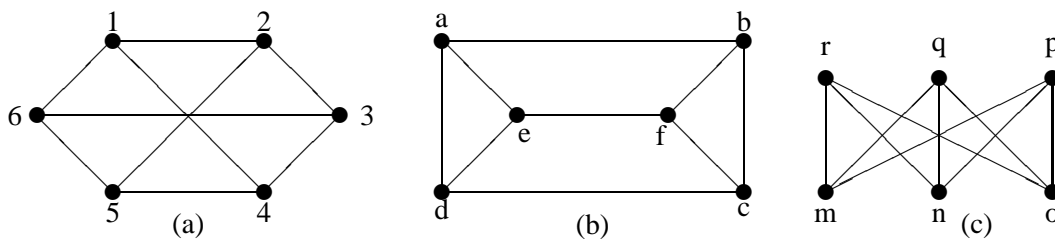


Figura 12.13: (G_1) , (G_2) , (G_3) grafos com mesma estrutura. (G_4) grafo com estrutura diferente de (G_1) , (G_2) e (G_3) .

O conceito de “mesma estrutura” pode ser formalizado da seguinte maneira. Dizemos que dois grafos G e H são *isomorfos* se existem bijeções $f : \mathcal{V}G \rightarrow \mathcal{V}H$ e $g : \mathcal{E}G \rightarrow \mathcal{E}H$ tais que um vértice v é extremo de uma aresta e no grafo G se e somente se $f(v)$ é extremo da aresta $g(e)$ no grafo H . No caso de grafos orientados, a direção da aresta tem que ser preservada também: a aresta e entra no (resp. sai do) vértice v em G se e somente se $g(e)$ entra em (resp. sai de) $f(v)$. Ou seja, as funções f e g preservam as relações de incidências entre vértices e arestas. Se os grafos são simples, é suficiente que exista uma função bijetora $f : \mathcal{V}G \rightarrow \mathcal{V}H$ que preserve as adjacências dos vértices. Se G e H são o mesmo grafo, dizemos que f é um *automorfismo* de G .

Escrevemos $G \cong H$ para indicar que G e H são isomorfos. Quando isto ocorre, qualquer propriedade de G que pode ser definida apenas em termos de incidências também será uma propriedade de H . Por esta razão, isomorfismo é um dos conceitos mais importantes da teoria dos grafos.

Exercício 12.29: Os grafos abaixo são isomorfos? Relacione-os dois a dois. Demonstre que são isomorfos, se o forem; caso contrário justifique porque não o são.



Dados dois grafos G e H , com $\mathcal{V}G = \mathcal{V}H = n$, verificar se G e H são isomorfos é um problema difícil. Uma maneira é na força bruta, ou seja analisar todas as $n!$ bijeções de $\mathcal{V}G$ para $\mathcal{V}H$ e verificar se alguma delas satisfaz a condição de isomorfismo. Há algoritmos mais

eficientes, mas todos os métodos conhecidos podem demorar demais em certos casos, mesmo para grafos relativamente pequenos.

É fácil provar (veja o exercício 12.30) que o isomorfismo é uma relação de equivalência entre grafos. Uma classe de equivalência desta relação é o conjunto de todos os grafos que tem um determinado diagrama (isto é, uma determinada estrutura), independentemente dos “rótulos” dos vértices e das arestas.

Por esse motivo, cada uma dessas classes é chamada de *grafo não rotulado*; e os grafos que vimos até agora podem então ser chamados de *grafos rotulados*. Este conceito se aplica a qualquer um dos tipos de grafos definidos na seção 12.3 (simples, orientado, etc.).

Pode-se verificar que todos os grafos simples completos com n vértices são isomorfos entre si. Portanto, para cada natural n , existe apenas um grafo não rotulado completo com n vértices, que é geralmente denotado por K_n .

As figuras 12.14 e 12.15 mostram todos os grafos simples (rotulados) com vértices $\{1, 2, 3\}$, e todos os grafos simples *não rotulados* com três vértices, respectivamente. Observe que vários dos grafos da figura 12.14 são isomorfos, e portanto correspondem ao mesmo diagrama da figura 12.15.

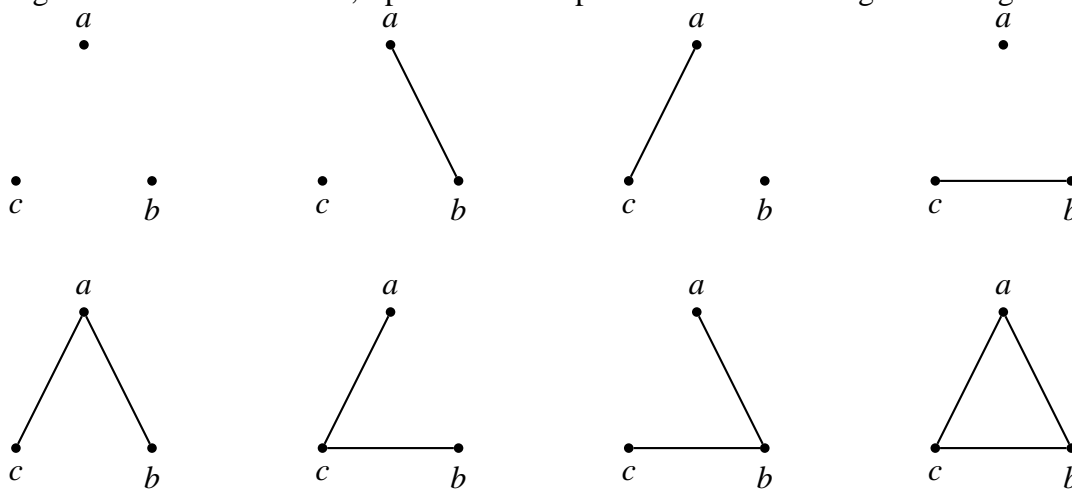


Figura 12.14: Grafos rotulados com três vértices.



Figura 12.15: Grafos não rotulados com três vértices.

Exercício 12.30: Prove que isomorfismo é uma relação de equivalência entre grafos.

Exercício 12.31: Prove que se G e H não são orientados e tem arestas paralelas, então $G \cong H$ se e somente se existe uma bijeção entre $\mathcal{V}G$ e $\mathcal{V}H$ que preserva adjacências: isto é, dois vértices u, v são adjacentes em G se e somente se $f(u)$ e $f(v)$ são adjacentes em H .

Exercício 12.32: Prove que a afirmação do exercício 12.31 não é verdade se G e G possuem arestas paralelas.

12.8.1 Contagem de grafos

Existem $2^{n(n-1)/2}$ grafos (orientados) simples com n vértices dados. Para justificar esta fórmula, basta observar que cada um dos $\binom{n}{2} = n(n-1)/2$ pares (ordenados) de vértices pode ser ou não aresta do grafo.

Se levarmos em conta isomorfismos — isto é, se contarmos grafos simples *não rotulados* com n vértices — o número é bem menor. Veja a tabela 12.1.

Tabela 12.1: Número de grafos simples com n vértices.

n	0	1	2	3	4	5	6	7	...
Rotulados	1	1	2	8	64	1.024	32.768	2.097.152	...
Não rotulados	1	1	2	4	34	156	1.044	12.346	...

A fórmula que permite calcular o número de grafos simples não rotulados com n vértices (a segunda linha da tabela 12.1) foi encontrada por George Pólya em 1935 [7, 8], mas é bastante complexa e foge do escopo deste livro.

12.9 Conexidade

12.9.1 Conexidade em grafos não orientados

Seja G um grafo não orientado. Dizemos que um vértice $u \in \mathcal{V}G$ está *conectado* ou *ligado* em G a um vértice $v \in \mathcal{V}G$ se e somente se existe um passeio em G com início u e término v . Isto equivale a dizer que existe um caminho em G de u para v (veja o exercício 12.15)

Dizemos que um grafo é *conexo* se ele não é vazio e quaisquer dois de seus vértices são conectados.

Exercício 12.33: Mostre que, em qualquer grafo não orientado G , a relação “está conectado a” é uma relação de equivalência.

Exercício 12.34: Sejam H e K dois subgrafos conexos de um grafo G . Demonstre que $H \cup K$ é conexo se e somente se $\mathcal{V}H \cap \mathcal{V}K \neq \emptyset$.

Exercício 12.35: Demonstre que um grafo G é conexo se e somente se existe um vértice $u \in \mathcal{V}G$ tal que todo vértice $v \in \mathcal{V}G$ está ligado a u .

As *componentes (conexas)* de um grafo G são os subgrafos conexos de G que são maximais na relação “ \subseteq ” (“é subgrafo de”). Uma propriedade importante das componentes é a seguinte:

Teorema 12.4: Um subgrafo H de um grafo não orientado G é uma componente conexa de G se e somente se H é conexo, e toda aresta de $\mathcal{E}G$ que tem um extremo em $\mathcal{V}H$ está em $\mathcal{E}H$ (e portanto tem os dois extremos em $\mathcal{V}H$).

Prova:

Para demonstrar a parte “somente se”, seja H uma componente conexa de G . Por definição, H é conexo. Seja e uma aresta qualquer de $\mathcal{E}G$ que tem uma ponta u em $\mathcal{V}H$. Seja v a outra ponta de e , e seja H' o subgrafo de G com vértices $\mathcal{V}H' = \mathcal{V}H \cup \{v\}$ e $\mathcal{E}H' = \mathcal{E}H \cup \{e\}$. O grafo H' é conexo, pois qualquer vértice $w \in \mathcal{V}H$ está conectado a u , e u está conectado a v pela aresta e . Mas, pela definição de componente, H é maximal dentre os subgrafos conexos de G sob \subseteq . Portanto, como $H \subseteq H'$, devemos ter $H = H'$; ou seja $e \in \mathcal{E}H$ e $v \in \mathcal{V}G$.

Para demonstrar a recíproca, suponha que H é um subgrafo conexo de G , e toda aresta de $\mathcal{E}G$ que tem um extremo em $\mathcal{V}H$ está em $\mathcal{E}H$. Vamos mostrar que H é maximal dentre os subgrafos conexos de G . Seja H' um subgrafo conexo de G tal que $H \subseteq H'$. Vamos mostrar que $H' = H$. Por definição de grafo conexo, H não é vazio. Seja portanto u um vértice de H , e v um vértice qualquer de H' . Como H' é conexo, existe um passeio $(v_0, e_1, v_1, \dots, v_n)$ em H' tal que $v_0 = u$ e $v_n = v$. Como e_1 tem uma ponta (u) em $\mathcal{V}H$, ela está em H e portanto a outra ponta v_2 está em $\mathcal{V}H$. Desta forma, por indução em i , provamos que v_i está em $\mathcal{V}H$ para todo i , e portanto v está em H . Concluimos assim que $\mathcal{V}H' = \mathcal{V}H$. Portanto, toda aresta $e \in \mathcal{E}H'$ tem as duas pontas em $\mathcal{V}H$; pela hipótese, e está em $\mathcal{E}H$, e concluimos que $\mathcal{E}H' = \mathcal{E}H$. Portanto $H' = H$, ou seja H é maximal.

Fim.

O teorema 12.4 implica que cada componente de um grafo G é essencialmente um grafo independente, sem intersecção ou ligação com as outras componentes.

Observe que um grafo é conexo se e somente se ele tem exatamente uma componente conexa. Em particular, o grafo vazio não é conexo. Alguns autores usam o termo *desconexo* para um grafo com duas ou mais componentes. Um grafo sem arestas é dito *totalmente desconexo*.

Seja e uma aresta de um grafo G . O grafo $G - e$ ou tem o mesmo número de componentes conexas que G , ou tem uma componente a mais. No segundo, caso dizemos que a aresta e é uma *aresta de corte*. Observe que, se retirarmos uma aresta de corte de um grafo conexo, obtemos um grafo desconexo.

Exercício 12.36: Seja G um grafo e u um vértice qualquer de G . Prove que a componente de G que contém u é $G[U]$, onde U é o conjunto de todos os vértices que estão ligados a u em G .

Exercício 12.37: Prove que uma aresta e de um grafo G é uma aresta de corte se e somente se e não pertence a nenhum ciclo de G .

12.9.2 Conexidade em grafos orientados

Um grafo orientado G é *fortemente conexo* se, para quaisquer dois vértices $u, v \in V$, existe um passeio orientado de u para v e de v para u . Isto equivale a dizer que existe um caminho orientado de u para v (veja o exercício 12.24.)

Um subgrafo fortemente conexos de um grafo orientado G que não está contido em nenhum outro subgrafo fortemente conexo de G é, por definição, uma *componente fortemente conexa* de

G . Isto é, as componentes fortemente conexas de G são os subgrafos fortemente conexas de G que são maximais sob “ \subseteq ”.

Ao contrário do que ocorre em grafos não orientados, uma componente fortemente conexa H de um grafo G não é necessariamente “isolada” das outras componentes. Pode existir uma (ou mais) aresta e de G que não está em $\mathcal{E}H$ mas tem origem ou destino em $\mathcal{V}H$. (Nesse caso é fácil provar que o outro extremo de e não está em $\mathcal{V}H$.)

Portanto, pode-se ver que as componentes fortemente conexas de um grafo orientado G não coincidem com as componentes conexas do grafo não orientado G' que é obtido de G ignorando-se as orientações das arestas. Em particular, se G' é conexo, G pode não ser fortemente conexo. Neste caso, diz-se que G é *fracamente conexo*.

12.10 Árvores

Uma *árvore* é um grafo conexo acíclico. Árvores são muito importantes, em computação e em outras áreas, e tem inúmeras propriedades interessantes. Por exemplo, a maneira mais econômica de interligar um conjunto de computadores e *switches* por cabos é formando uma árvore.

Observe que uma árvore é necessariamente um grafo simples.

Teorema 12.5: Em uma árvore quaisquer dois vértices são ligados por um único caminho.

Prova:

Sejam T uma árvore e u e v dois vértices de T . Como T é conexo existe um caminho P ligando o vértice u ao vértice v . Suponhamos, por contradição, que este caminho não é único, ou seja, existe um caminho Q , distinto de P ligando o vértice u ao vértice v . Como os caminhos são distintos existe uma aresta e que ocorre em P e não em Q . Podemos escrever então $P = P_1 \cdot (x, e, y) \cdot P_2$ onde x e y são os extremos de e . Considere agora o subgrafo H de G que consiste de todos os vértices e arestas de P e de Q , exceto a aresta e . A concatenação $P_1^{-1} \cdot Q \cdot P_2^{-1}$ é um passeio que visita todos os vértices de H . Portanto H é conexo. Logo existe um caminho R em H de x para y que não passa por e . A concatenação $R \cdot (y, e, x)$ é portanto um circuito em T . Isto contradiz a definição de árvore. Portanto concluímos que o caminho P é único.

Fim.

Outra propriedade de árvores que precisaremos mais adiante é a seguinte:

Corolário 12.6: Seja G uma árvore e e uma aresta de G . O grafo $G \setminus \{e\}$ tem exatamente duas componentes conexas.

Prova:

Sejam u e v os extremos de e , e seja $H = G \setminus \{e\}$. Pelo teorema 12.5, o único caminho entre u e v em G é (u, e, v) . Portanto em H não existe caminho entre u e v , implicando que H é desconexo.

Por outro lado, todo vértice x de G está ligado a u por um único caminho $P(x)$. Se esse caminho não passa por e , então ele é um caminho em H . Se ele passa por e , então

$P(x) = P'(x) \cdot (v, e, u)$, e portanto $P'(x)$ é um caminho de x para v em H . Concluímos que todo vértice de H está ligado em H ao vértice u ou ao vértice v . Portanto H tem exatamente duas componentes conexas: a que contém u , e a que contém v .

Fim.

Este corolário implica que toda aresta de uma árvore é uma aresta de corte.

Teorema 12.7: Seja G uma árvore com $|\mathcal{V}G| = n$ e $|\mathcal{E}G| = m$ então $m = n - 1$.

Prova:

Vamos provar este teorema por indução no número de vértices. Observe que, como um grafo conexo não pode ser vazio, uma árvore tem pelo menos um vértice.

- *Base:* Se $n = 1$, então qualquer aresta de G seria um laço, e portanto formaria um circuito. Portanto G tem zero arestas, e a afirmação é verdadeira.
- *Hipótese de indução:* Para todo $k < n$, uma árvore com k vértices tem $k - 1$ arestas.
- *Passo:* Supondo que $n \geq 2$ e a hipótese de indução, vamos provar que toda árvore G com n vértices tem $n - 1$ arestas. Como G é conexo, ele deve ter pelo menos uma aresta $e = (u, v)$. Considere o subgrafo $H = G \setminus \{e\}$. Pelo lema 12.6, H tem exatamente duas componentes conexas, H_1 e H_2 . Sejam $n_1 = |\mathcal{V}H_1|$ e $n_2 = |\mathcal{V}H_2|$; note que $n_1 + n_2 = n$, $n_1 < n$, e $n_2 < n$. Portanto, pela hipótese de indução, H_1 tem $n_1 - 1$ arestas, e H_2 tem $n_2 - 1$ arestas. Logo o número de arestas de G é $(n_1 - 1) + (n_2 - 1) + 1 = n_1 + n_2 - 1 = n - 1$.

Fim.

12.11 Grafos bipartidos

Seja $G = (\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$ um grafo. Uma *bipartição* de $\mathcal{V}G$ é um par não ordenado de subconjuntos \mathcal{V}^-GG e \mathcal{V}^+GG de $\mathcal{V}G$, tais que $\mathcal{V}^-GG \cup \mathcal{V}^+GG = \mathcal{V}G$ e $\mathcal{V}^-GG \cap \mathcal{V}^+GG = \emptyset$ e toda aresta do grafo tem um extremo em \mathcal{V}^-GG e o outro em \mathcal{V}^+GG . Um grafo G com uma bipartição $\mathcal{V}^-GG, \mathcal{V}^+GG$ é chamado um *grafo bipartido*.

Um *grafo bipartido completo* é um grafo bipartido no qual todo vértice de \mathcal{V}^-GG é adjacente a todo vértice de \mathcal{V}^+GG .

Verifica-se que uma condição necessária e suficiente para que um grafo $G = (\mathcal{V}G, \mathcal{E}G, \mathcal{F}G)$ tenha uma bipartição é que ele não possua ciclos de comprimento ímpar.

Pode-se verificar (veja o exercício 12.38) que, para cada par de números naturais m e n , existe apenas um grafo não rotulado bipartido completo cuja bipartição tem m vértices em um conjunto e n vértices no outro. Esse grafo não rotulado é geralmente denotado por $K_{m,n}$.

Exercício 12.38: Mostre que dois grafos bipartidos completos G e H são isomorfos se e somente se existirem bipartições $\mathcal{V}^-G, \mathcal{V}^+G$ de G e $\mathcal{V}^-H, \mathcal{V}^+H$ de H tais que $\#\mathcal{V}^-G = \#\mathcal{V}^-H$ e $\#\mathcal{V}^+G = \#\mathcal{V}^+H$.

Exercício 12.39: Quando é que um grafo bipartido completo é regular?

12.12 Grafos eulerianos

Para mostrar que o problema das pontes de Königsberg não tem solução, Euler primeiro modelou o mapa da figura 12.2 por um grafo G não orientado, onde cada vértice representava uma região de terra firme (uma margem do rio ou uma ilha), e cada aresta representava uma ponte entre as duas regiões representadas pelos seus extremos. Veja figura 12.16. Neste modelo, o problema pede um passeio no grafo G que atravessa exatamente uma vez cada aresta de $\mathcal{E}G$; ou seja, uma trilha que atravessa por todas as arestas. Uma trilha com esta propriedade é chamada de *trilha euleriana* ou *trilha de Euler* do grafo G . Se a trilha é fechada ela é chamada de *tour euleriano* ou *tour de Euler*. Um grafo é dito *euleriano* se ele contém um tour de Euler.

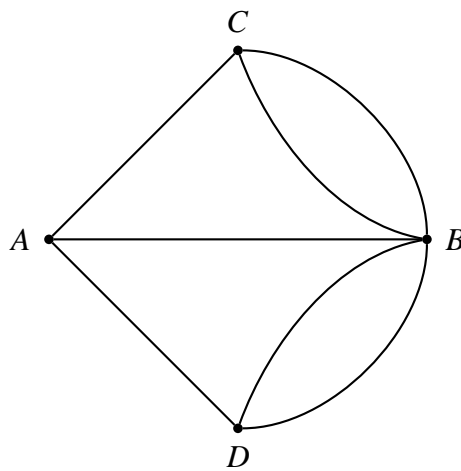


Figura 12.16: Grafo das pontes de Königsberg

No seu artigo de 1736, Euler fez mais do que resolver o problema da cidade de Königsberg. Ele encontrou uma condição necessária e suficiente para que um grafo qualquer G tenha um tour euleriano:

Teorema 12.8: Um grafo conexo tem um tour de Euler se e somente se ele não tem vértices de grau ímpar.

A demonstração da parte “somente se” do teorema é o exercício 12.41. A prova da parte “se” do enunciado é mais trabalhosa e foge do escopo deste livro.

Outro quebra-cabeças clássico que recai no mesmo problema de grafos é desenhar cada um dos diagramas da figura 12.17 sem levantar o lápis do papel e sem traçar duas vezes a mesma linha. Cada desenho pode ser modelado por um grafo G , onde os vértices são os extremos isolados de linhas ou pontos onde três ou mais linhas se encontram; e as arestas são as linhas ligando esses pontos. Nesse caso, o que se pede é uma *trilha euleriana*, uma trilha (não necessariamente fechada) que passa por todas as arestas de G . O seguinte teorema é um corolário do teorema de Euler:

Corolário 12.9: Um grafo conexo tem uma trilha de Euler se e somente se ele tem no máximo dois vértices de grau ímpar.

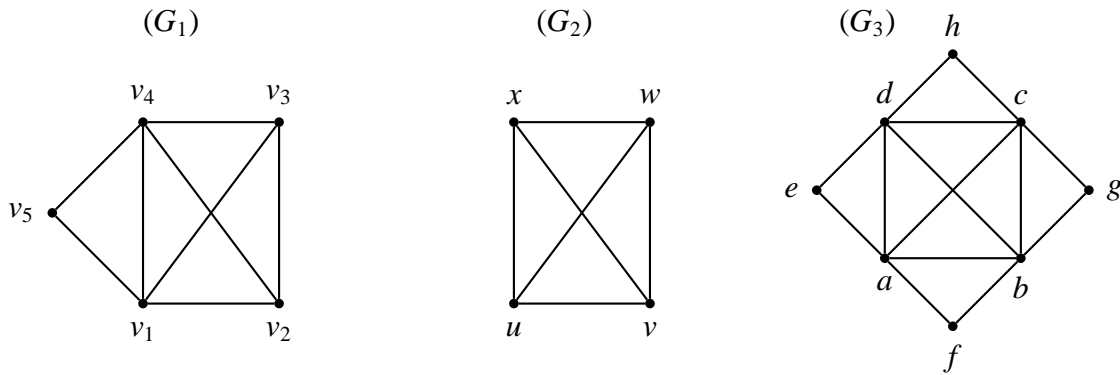


Figura 12.17: Grafos com trilhas eulerianas.

Exercício 12.40: Para que valores de n um grafo completo com n vértices tem um tour de Euler?

Exercício 12.41: Seja G um grafo conexo. Se G tem um tour de Euler então G não tem vértices de grau ímpar.

12.13 Grafos hamiltonianos

Considere o seguinte quebra-cabeças: o Rei Artur precisa designar os assentos para seus 24 Cavaleiros em volta da Távola Redonda. Mas nem todos eles são amigos; e é importante que cada cavaleiro seja colocado entre dois de seus amigos.

Podemos descrever as relações de amizade como um grafo simples G onde os vértices são os Cavaleiros e existe uma aresta entre dois Cavaleiros se eles são amigos (e portanto podem sentar lado a lado). Veja por exemplo a figura 12.18.

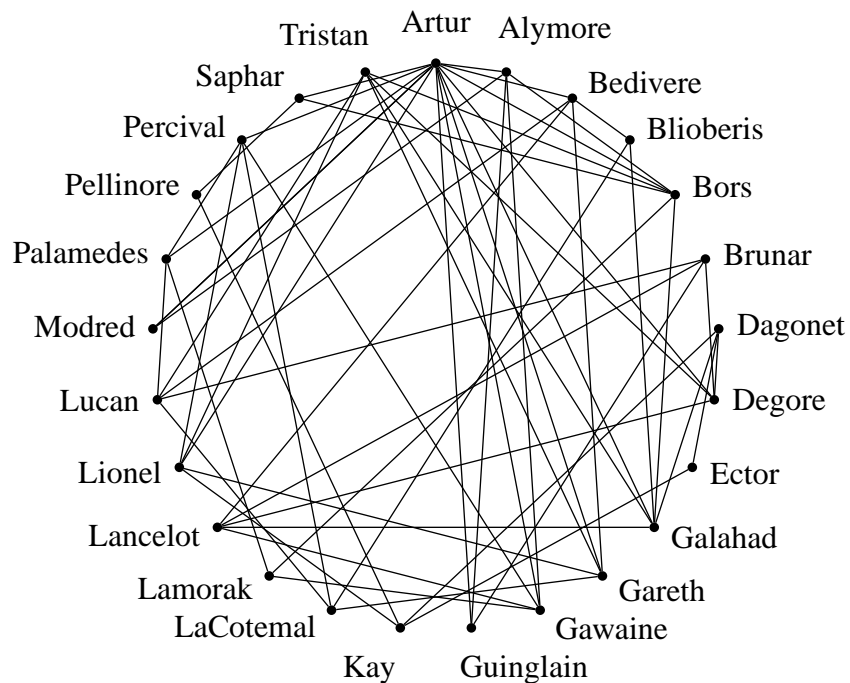


Figura 12.18: O grafo de amizades dos Cavaleiros da Távola Redonda.

Pode-se ver que a solução do quebra-cabeças é um circuito nesse grafo G que passa por todos os seus vértices; ou seja, um passeio fechado que passa exatamente uma vez em cada vértice. Veja a figura 12.19.

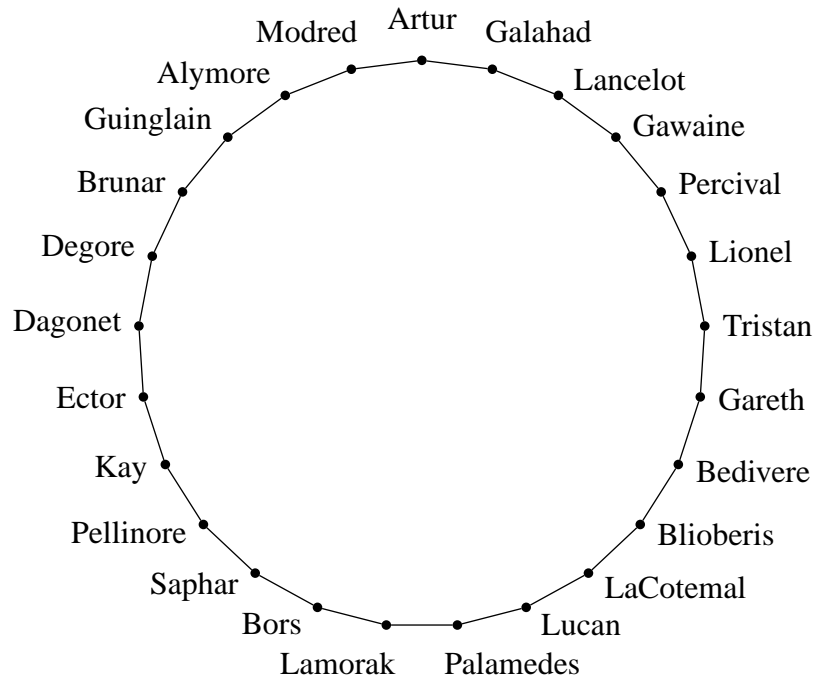


Figura 12.19: Uma solução para o problema do Rei Artur.

Um circuito com essas propriedades é chamado de *circuito hamiltoniano* do grafo G . Este nome homenageia o matemático irlandês William Rowland Hamilton (1805–1861). Em 1856 ele descreveu, em uma carta a um colega, um jogo para duas pessoas baseado no grafo G da figura 12.20, derivado do dodecaedro. Nesse jogo, uma pessoa escolhe um caminho P qualquer de cinco vértices no grafo G , e a outra deve encontrar um circuito em G que começa com P e passa por todos os vértices.

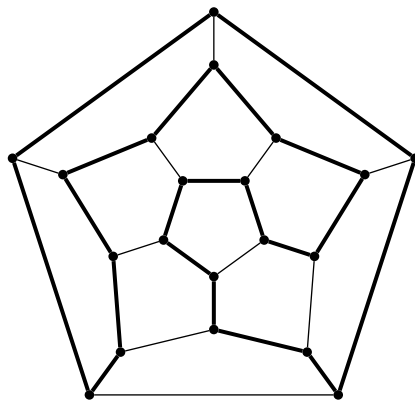


Figura 12.20: O grafo G do jogo de Hamilton.

Um grafo que possui pelo menos um circuito hamiltoniano é chamado de *grafo hamiltoniano*. A figura 12.21 mostra alguns exemplos de grafos hamiltonianos (com os respectivos circuitos) e de grafos não hamiltonianos.

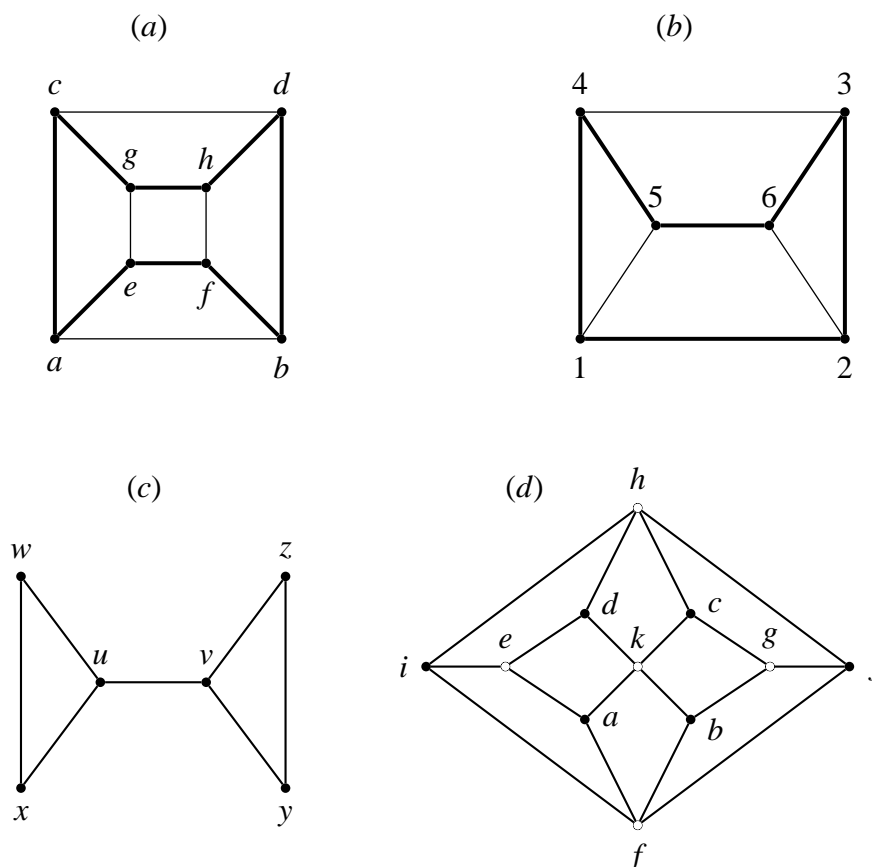


Figura 12.21: (a) e (b) grafos hamiltonianos. (c) e (d) grafos não hamiltonianos.

Há vários argumentos que podem ser usados para demonstrar que um grafo não é hamiltoniano. Por exemplo, se G tem um vértice de grau 1, então G não é hamiltoniano. No exemplo da figura 12.21(c), pode-se ver que qualquer passeio que visite os vértices u e v deve repetir a aresta a , e portanto não pode ser um circuito. No exemplo da figura 12.21(d), pode-se observar que os cinco vértices brancos e os seis vértices pretos formam uma bipartição $\mathcal{V}^- G, \mathcal{V}^+ G$ de G . Como os dois conjuntos tem cardinalidades diferentes, podemos concluir que não há circuito que passe por todos os vértices.

Um grafo completo K_n sempre tem um circuito hamiltoniano se $n \geq 3$. Uma condição suficiente para um grafo G seja hamiltoniano é que $|\mathcal{V}G| \geq 3$ e cada vértice tenha grau pelo menos $\lfloor \mathcal{V}G \rfloor / 2$. Entretanto, esta condição não é necessária. A demonstração deste teorema (e muitas outras condições necessárias ou suficientes para um grafo ser hamiltoniano) pode ser encontrada em textos de teoria de grafos [2, 3].

Em contraste com os grafos eulerianos, não se conhece nenhum algoritmo eficiente para encontrar um circuito hamiltoniano em um grafo G dado. Na verdade, não se conhece nenhuma condição necessária e suficiente para saber se um grafo é hamiltoniano que seja fácil de testar.

Um caminho que visita todos os vértices de um grafo G é chamado *caminho hamiltoniano* de G .

Exercício 12.42: Um cofre tem uma fechadura elétrica acionada por três chaves, cada uma das quais pode estar em duas posições indicadas por ‘0’ e ‘1’. A porta abre somente se as três chaves estiverem em uma combinação secreta específica, por exemplo ‘011’. Um ladrão que não conhece o segredo quer tentar todas as combinações mexendo em apenas uma chave de cada vez, no menor tempo possível. Modele o problema em um grafo e encontre uma solução para o mesmo. Faça o mesmo para um cofre com quatro chaves.

Exercício 12.43: Um *poliedro* é um sólido geométrico limitado por polígonos planos. A todo poliedro K corresponde um grafo G tal que $\mathcal{V}G$ é o conjunto dos vértices (cantos) de K , $\mathcal{E}G$ é o conjunto das arestas (quinas) de P , e as pontas de cada aresta em G são as mesmas em G e em K .

Os *poliedros platônicos* são poliedros cujas faces, vértices, arestas e ângulos são todos iguais. Existem apenas sete poliedros platônicos: o tetraedro, o cubo, o octaedro, o icosaedro, e o dodecaedro regulares. Desenhe os grafos desses poliedros, e determine quais deles possuem um circuito hamiltoniano,

Exercício 12.44: Dê exemplos de:

1. Um grafo euleriano que não é hamiltoniano.
2. Um grafo hamiltoniano que não é euleriano.

Exercício 12.45: Demonstre que se G é um grafo bipartido com um número ímpar de vértices, então G não é um grafo hamiltoniano.

Exercício 12.46: Considere um tabuleiro de xadrez. Um cavalo pode, através de seus movimentos no jogo de xadrez, passar por todas as casas do tabuleiro e retornar à casa de onde partiu? Responda esta questão considerando um “tabuleiro” 4×4 , 5×5 , 7×7 , 8×8 . Sugestão: O exercício 12.45 poderá auxiliar em alguns desses casos.

Exercício 12.47: Prove, por indução, que o n -cubo é um grafo hamiltoniano.

12.14 Grafos planares

Um quebra-cabeças clássico pede para ligar três casas a três centrais de serviço — água, esgoto e internet banda-larga — sem que nenhuma dessas ligações cruze qualquer outra. Veja a figura 12.22.

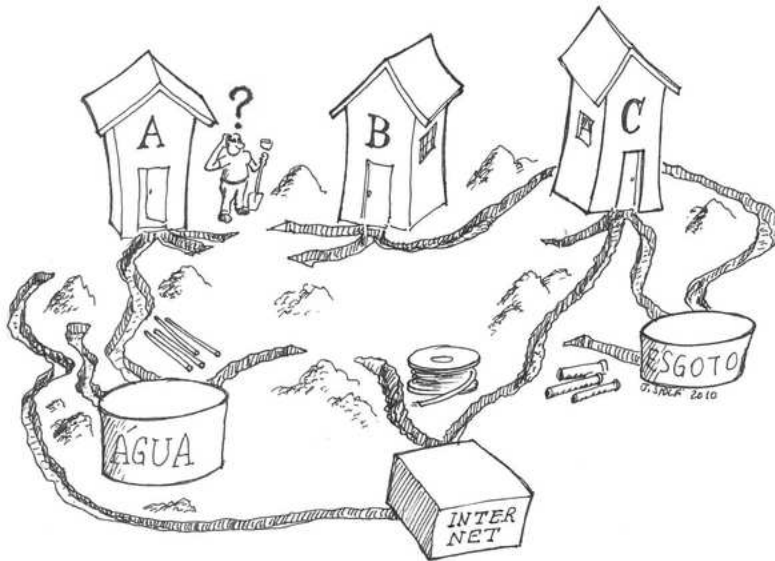


Figura 12.22: O problema das três casas e três serviços.

O problema pede para desenhar um grafo G (neste caso, o grafo completo bipartido $K_{3,3}$) no plano, de modo que nenhuma aresta cruze outra aresta ou passe por um vértice que não é seu extremo. Um desenho deste tipo é chamado de *representação planar* do grafo G . Se G pode ser desenhado desta forma, dizemos que ele é um grafo *planar*.

Nem todo grafo é planar. A figura 12.23 mostra exemplos de grafos planares e não planares.

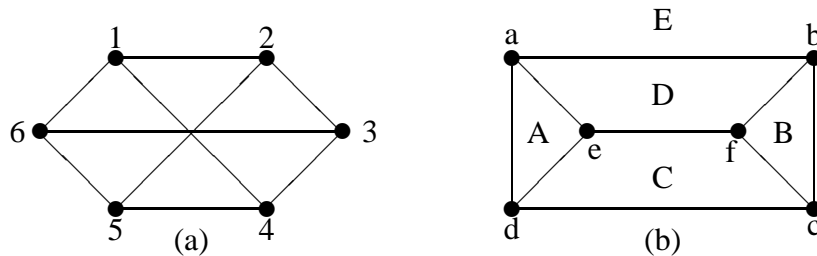


Figura 12.23: (a) Um grafo não planar. (b) Um grafo planar.

Uma representação planar de um grafo divide o plano em uma ou mais regiões, separadas pelos desenhos dos vértices e arestas. Essas regiões são chamadas de *faces* da representação. Na figura 12.23(b), há cinco faces (A, B, C, D, E). Note que uma dessas regiões — a *face externa* E — tem tamanho infinito; as demais tem tamanho finito.

A teoria dos grafos planares é bastante extensa e necessita de conhecimentos de topologia do espaço \mathbb{R}^2 que fogem ao escopo deste livro. Portanto indicaremos apenas alguns resultados importantes sobre este tema, sem demonstração.

Teorema 12.10: Seja \hat{G} uma representação planar de um grafo G . Uma aresta e de G pertence a um circuito se e somente se ela separa duas faces distintas de \hat{G} .

Corolário 12.11: Um grafo é uma árvore se e somente se ele tem uma representação planar com uma única face.

12.14.1 A fórmula de Euler para grafos planares

Um mesmo grafo planar G pode ter várias representações planares bem diferentes. Na figura 12.24, por exemplo, no primeiro desenho as faces A, B, C, D tem 3, 3, 5 e 5 lados, respectivamente, enquanto que no segundo as faces A', B', C', D' tem 3, 3, 4 e 6 lados, respectivamente.

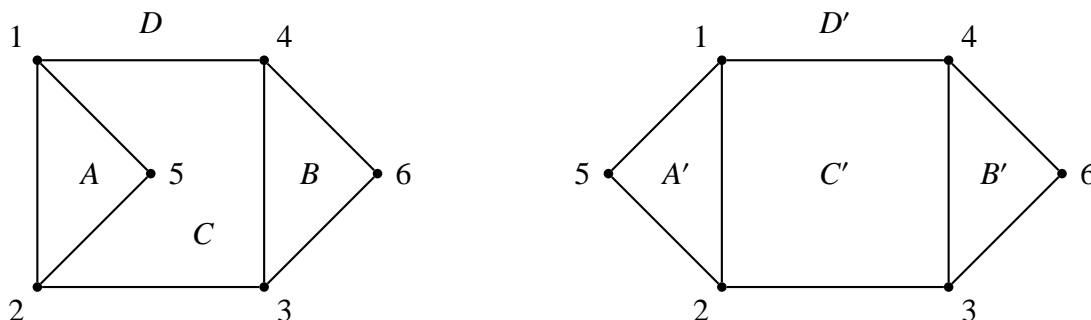


Figura 12.24: Duas representações planares do mesmo grafo.

No entanto, Euler descobriu que toda representação planar de um mesmo grafo G tem o mesmo número de faces. Este resultado foi expresso pelo seguinte teorema:

Teorema 12.12:[Fórmula de Euler] Seja \hat{G} uma representação planar de um grafo simples e conexo G . Seja f o número de faces de \hat{G} . Então $f = e - v + 2$, onde $v = |\mathcal{V}G|$ e $e = |\mathcal{E}G|$.

Prova:

Vamos provar usando indução no número de faces de \hat{G} . Se $f = 1$ então, pelo teorema 12.11, G é uma árvore. Nesse caso, pelo teorema 12.7, temos $e = v - 1$. Portanto o enunciado vale para $f = 1$.

Suponhamos agora que f é um inteiro maior ou igual a 2, e que a afirmação é verdadeira para todas as representações planares de grafos simples com o número de faces menor que f . Seja \hat{G} uma representação de um grafo conexo e planar G com f faces. Escolha uma aresta a de G que não seja uma aresta de corte. Logo a pertence a algum circuito de G (veja o exercício 12.37), e portanto, pelo teorema 12.10, ela separa duas faces distintas de \hat{G} . Então retirando a aresta a de \hat{G} obtemos uma representação \hat{G}' do subgrafo $G - a$. Observe que $G - a$ é conexo e que \hat{G}' tem $f' = f - 1$ faces, pois as duas faces de \hat{G} separadas por a tornam-se uma face em \hat{G}' . Sejam $v' = v$ e $e' = e - 1$ o número de vértices e arestas do grafo $G - a$. Por hipótese de indução temos que

$$f' = e' - v' + 2$$

ou seja

$$(f - 1) = (e - 1) - v + 2$$

e portanto

$$f = e - v + 2$$

Fim.

Uma consequência da fórmula de Euler é que um grafo planar não pode ter muitas arestas. Mais precisamente:

Corolário 12.13: Seja G um grafo planar, simples e conexo, com pelo menos três vértices. Então $|\mathcal{E}G| \leq 3|\mathcal{V}G| - 6$.

O corolário 12.13 permite concluir que o grafo completo K_5 não é planar, pois para ele temos $|\mathcal{V}K_5| = 5$, $|\mathcal{E}K_5| = 10$, e $10 > 3 \cdot 5 - 6 = 9$.

Corolário 12.14: Seja G um grafo planar, simples e conexo, com pelo menos três vértices. Se G não possui ciclos de comprimento 3, então $|\mathcal{E}G| \leq 2|\mathcal{V}G| - 4$.

Este corolário permite concluir que $K_{3,3}$ não é planar, pois ele não tem ciclos de comprimento 3, tem $|\mathcal{V}K_{3,3}| = 6$, $|\mathcal{E}K_{3,3}| = 9$, e $9 > 2 \cdot 6 - 4 = 8$. Observe que este resultado mostra que o problema das três casas e três serviços não tem solução.

12.14.2 O teorema de Kuratowski

A definição de grafo planar usa o conceito de curvas desenhadas no plano \mathbb{R}^2 , e portanto sai do domínio da matemática discreta (grafos) para o domínio da matemática contínua (geometria e topologia do plano). Entretanto, em 1930, o matemático polonês Kasimierz Kuratowski (1896–1980) descobriu que é possível caracterizar os grafos planares apenas em termos discretos.

Para apresentar esse resultado precisamos do conceito de *subdivisão de um grafo*. Dizemos que um grafo simples H é uma *subdivisão* de outro grafo simples G se $\mathcal{V}G \subseteq \mathcal{V}H$, e para cada aresta $e \in \mathcal{E}G$ existe um caminho C_e em H ligando os extremos e ; sendo que toda aresta de $\mathcal{E}H$ e todo vértice de $\mathcal{V}H \setminus \mathcal{V}G$ ocorre em exatamente um destes caminhos. (Ou seja, se e somente se H pode ser obtido de G inserindo-se zero ou mais vértices novos ao longo de cada aresta.) Veja a figura 12.25.

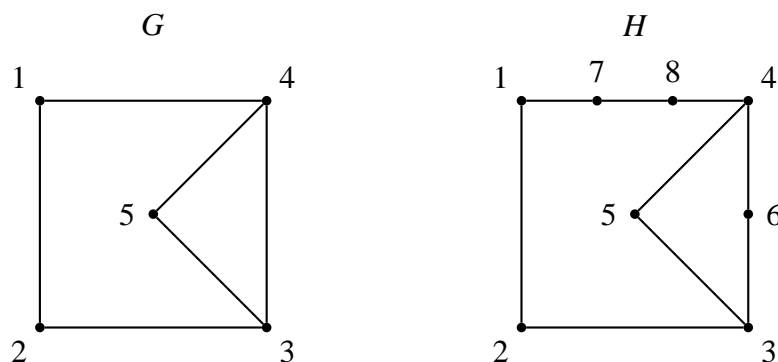


Figura 12.25: Um grafo G e uma subdivisão H de G .

Teorema 12.15:[Teorema de Kuratowski] Um grafo G é planar se e somente se ele não contém um subgrafo que seja isomorfo a uma subdivisão do K_5 ou do $K_{3,3}$.

Exemplo 12.1: A figura 12.26(a) mostra o chamado *grafo de Petersen* (estudado pelo matemático dinamarquês Julius Petersen, 1839–1910) que denotaremos por P . Seja H o subgrafo de P formado pelos vértices e arestas cheias, que está redesenhado na figura 12.26(b). Neste desenho é fácil ver que H é isomorfo a uma subdivisão do grafo completo $K_{3,3}$ ilustrado na figura 12.26(c). Note, por exemplo, que o caminho (e, a, f) de H corresponde à aresta $(1, 4)$ de $K_{3,3}$.

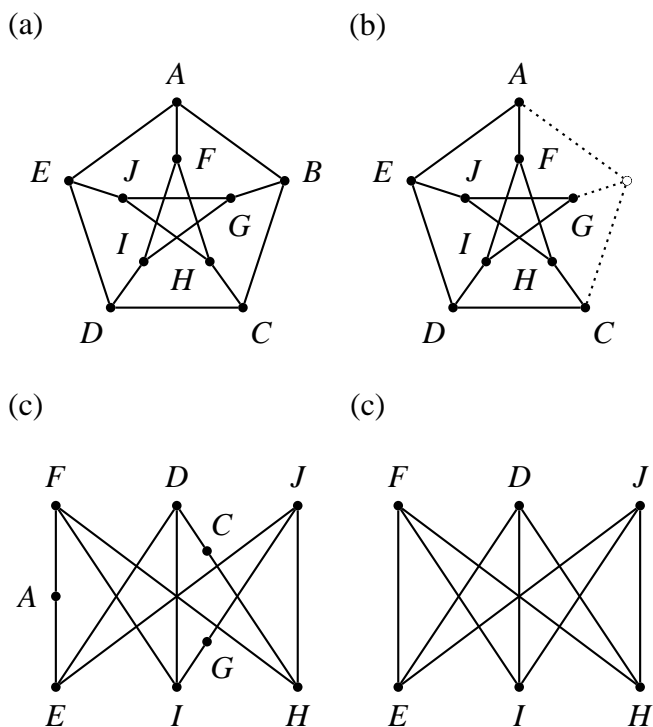


Figura 12.26: (a) o grafo de Petersen. (b,c) O subgrafo $G \setminus \{B\}$ desenhado de duas maneiras diferentes. (c) um grafo $K_{3,3}$ que subdividido dá $G \setminus \{B\}$.

Exercício 12.48: Assinale com **V** ou **F** as afirmações que são verdadeiras ou falsas respectivamente:

- todo subgrafo de um grafo planar é planar.
- todo subgrafo de um grafo não-planar é não-planar.
- todo grafo que contém um grafo planar (como subgrafo) é planar.
- todo grafo que contém um grafo não-planar (como subgrafo) é não-planar.

Exercício 12.49: Para que valores de n , K_n é planar?

Exercício 12.50: Para quais valores de r e s ($r \leq s$) o grafo bipartido completo $K_{r,s}$ é planar?

12.14.3 Grafo dual

Seja \hat{G} é uma representação planar de um grafo G , e seja H um grafo definido da seguinte maneira:

- Os vértices de H são as faces de \hat{G} ;
- As arestas de H são as arestas de G ;
- Uma aresta e tem extremos nos vértices A e B em H se e somente se ela é parte da fronteira entre as faces A e B em \hat{G} .

Verifica-se que H também é um grafo planar, e tem uma representação planar \hat{H} tal que cada vértice de \hat{H} está dentro da face correspondente de \hat{G} , e vice-versa; e tal que uma aresta e' em \hat{H} cruza uma aresta e'' de \hat{G} se e somente se $e' = e''$. Veja a figura 12.27. Neste caso, diz-se que \hat{G} e \hat{H} são *representações planares duais*, e que G e H são *grafos duais*.

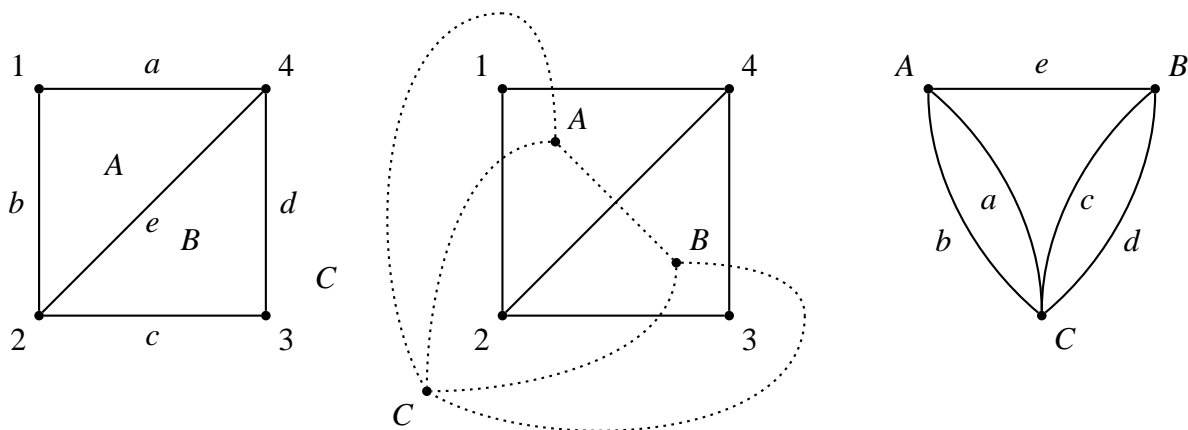


Figura 12.27: Uma representação planar \hat{G} de um grafo G (esq.) e sua representação planar dual \hat{H} (dir.).

Para cada afirmação sobre uma representação planar \hat{G} há uma afirmação equivalente sobre a representação dual \hat{H} , onde os conceitos de face e vértice trocam de papéis. Por exemplo, dizer que \hat{G} possui um vértice de grau 5 equivale a dizer que \hat{H} possui uma face com cinco lados (levando em conta que uma mesma aresta pode contribuir dois lados). Aplicando esta correspondência a teoremas já provados podemos obter outros teoremas, às vezes nada óbvios, que não precisam ser demonstrados.

12.15 Coloração de grafos

12.15.1 Coloração de mapas

É costume em mapas pintar os países (estados, municípios, etc) com cores variadas, de tal forma que estados que tem fronteira comum tenham cores diferentes — a fim de tornar as fronteiras

mais visíveis. Uma questão antiga é quantas cores diferentes são necessárias para esse fim. A experiência sugere que três cores são insuficientes, mas quatro cores bastam (desde que cada país seja um único território contínuo). Será que existe algum mapa que precisa de cinco (ou mais) cores?

Em 1852 esta questão foi colocada como um problema matemático pelo aluno inglês Francis Guthrie (1831–1899), e foi amplamente divulgada pelo seu professor Augustus De Morgan. Em 1879, o matemático inglês Alfred Kempe (1849–1922) publicou uma demonstração de que quatro cores eram suficientes. Porém, em 1890 foi observado que havia uma falha na demonstração de Kempe. Uma demonstração correta foi obtida apenas em 1976, por Kenneth Appel e Wolfgang Haken. Essa demonstração causou bastante controvérsia, pois os autores reduziram o problema a 2000 casos separados, e utilizaram um programa de computador para enumerar e verificar todos esses casos. Por esse motivo muitos matemáticos se recusaram a considerar a demonstração válida, e ela foi publicada somente em 1989. Em 1996 Robertson, Sanders, Seymour e Thomas conseguiram simplificar a demonstração reduzindo a lista para “apenas” 633 casos. (Hoje demonstrações usando computador tornaram-se ferramentas importantes em matemática.)

Um mapa de países pode ser visto como uma representação planar \hat{G} de um grafo G : cada vértice de G é um ponto do mapa onde três ou mais países tem fronteira comum, e cada aresta é um trecho de fronteira entre dois países ligando dois desse pontos. Na representação dual \hat{H} de \hat{G} , cada vértice é um país, e existe uma aresta ligando dois países se e somente se eles tem um trecho de fronteira em comum. Portanto, o resultado de Appel e Haken pode ser reformulado como segue

Teorema 12.16:[Teorema das quatro cores] Se H é um grafo planar, é sempre possível colorir seus vértices com quatro cores, de modo que quaisquer dois vértices adjacentes tenham cores distintas.

12.15.2 Coloração de grafos em geral

O problema das quatro cores é um caso particular de uma questão mais geral sobre grafos arbitrários (não necessariamente planares).

Definimos uma k -coloração de um grafo simples G como uma atribuição de k cores aos vértices de tal forma que vértices adjacentes não tem a mesma cor. O número cromático de G é o menor número k de cores tal que G tem uma k -coloração. Denotaremos por $\chi(G)$ o número cromático de um grafo G .

É fácil ver que o número cromático de G é 2 se e somente se G é bipartido, e que o número cromático do grafo completo K_n é n . O teorema das quatro cores diz que o número cromático de um grafo planar é no máximo 4.

Ainda não se conhece um algoritmo eficiente para determinar o número cromático de um grafo simples G arbitrário. Entretanto, existe um teorema que limita o número a um intervalo bem reduzido:

Teorema 12.17: Seja G um grafo simples, e Δ o maior dos graus de seus vértices. O número cromático de G é no máximo $\Delta + 1$.

Exercício 12.51: Qual é o número cromático do grafo ciclo com cinco vértices (C_5)? E do grafo ciclo com n vértices (C_n) em geral?

Exercício 12.52: Qual é o número cromático do grafo completo bipartido $K_{p,q}$, para $p, q \geq 1$?

Exercício 12.53: Seja G um grafo com pelo menos uma aresta. Prove que G é um grafo bipartido se, e somente se, o número cromático de G é dois.

Exercício 12.54: Seja G um grafo planar com n vértices. Prove, usando indução, que os vértices de G podem ser pintados com 6 cores.

Exercício 12.55: Prove o teorema 12.17 usando indução no número de vértices do grafo.

Capítulo 13

Probabilidade

A lógica é uma ferramenta essencial pois nos permite deduzir o valor lógico de proposições mais complexas a partir dos valores lógicos de suas proposições e predicados elementares. Porém, para usá-la precisamos saber se as proposições e predicados são verdadeiros ou falsos.

Na vida real, é raro sabermos com certeza se uma afirmação é verdadeira ou não. Todas as fontes de informação que temos — notícias, contagens, medidas, evidências, e nossos próprios sentidos e mente — podem ser errôneas ou enganosas; de modo que toda proposição que acreditamos verdadeira pode ser falsa, e vice-versa. Como podemos então usar a lógica, ou tomar qualquer decisão, nessas condições?

Por outro lado, há afirmações sobre as quais temos muito mais confiança do que outras. Podemos tratar a frase “ontem choveu na minha rua” como verdadeira, com confiança quase absoluta, se estávamos lá ontem. Por outro lado, se a previsão do tempo diz que “não vai chover amanhã”, é prudente pensar na possibilidade que chova.

Para certas afirmações, nossa confiança pode vir do histórico de situações semelhantes que já presenciamos. Podemos tratar como certa a proposição “uma pedra solta no ar cai para baixo” com base em incontáveis experiências que tivemos ao longo da vida. As leis da física, em particular, são “certezas” adquiridas por meio de experimentos cuidadosos e exaustivamente analisados. Mesmo assim sempre é possível que, em situações especiais que nunca encontramos antes, essas afirmações “certamente verdadeiras” venham a ser falsas.

Para algumas proposições, nossa confiança pode se dividir igualmente entre as duas possibilidades. Alguém jogou uma moeda ao ar e ela caiu onde não podemos ver. Será que o resultado foi cara, ou coroa? Nossa experiência com moedas nos diz que às vezes o resultado é um, às vezes é outro. Da mesma forma, quando atiramos um dado, nossa experiência diz apenas que o resultado pode ser qualquer número entre 1 e 6, e que parece não haver diferença entre eles. Por essa experiência, afirmação “o resultado será 3” merece tanta confiança quanto “o resultado será 5”. Na verdade, jogos de azar como dados e cara-ou-coroa baseiam-se inteiramente no fato de que todos resultados possíveis são igualmente plausíveis.

Por outro lado, mesmo nesses jogos há afirmações que merecem mais confiança do que outras. Quando atiramos um dado, a afirmação “o resultado será 3” deve nos parecer menos plausível do que “o resultado será diferente de 3”. Esta confiança pode vir da experiência, mas também por raciocínio: se todos os 6 resultados tem chances iguais de acontecer, então o resultado 3 deve ter menos chances do que os outros cinco juntos.

A teoria da probabilidade surgiu para formalizar este tipo de raciocínio, que tem o mesmo

objetivo da lógica clássica — ajudar-nos a pensar e decidir — mas lida com graus de confiança, em vez de certezas absolutas.

13.1 Definição

Nesta teoria, cada proposição P tem uma *probabilidade*: um valor real entre 0 e 1, que mede o grau de confiança ou expectativa que temos de que a proposição seja verdadeira. Denotaremos esse número por $\text{Pr}(P)$. Probabilidade 1 significa que temos certeza absoluta de que a afirmação P é verdadeira. Probabilidade 0 significa que temos certeza absoluta que é falsa. O valor $1/2$ significa que não sabemos se P é falsa ou verdadeira, e que qualquer das duas possibilidades nos parece igualmente provável. Assim, por exemplo, quando vamos jogar uma moeda, podemos atribuir probabilidade $1/2$ à afirmação “o resultado será cara”. Uma probabilidade mais próxima de 1 significa que não temos certeza, mas acreditamos que é mais provável que a afirmação P seja verdadeira do que ela seja falsa.

Na teoria de da probabilidade, toda proposição P em tese continua tendo um valor lógico “verdadeiro” ou “falso”, mas a teoria não exige que esse valor seja conhecido. A probabilidade da afirmação reflete justamente nosso grau de conhecimento. Se conhecemos o valor lógico da afirmação, devemos atribuir a ela probabilidade 0 ou 1; e, nesse caso, como veremos, a teoria da probabilidade se reduz à lógica clássica.

As probabilidades são frequentemente expressas em percentagens. Assim, tanto faz dizer que uma probabilidade é 25% ou $25/100 = 0,25$.

13.1.1 Distribuição uniforme

Em geral, quando temos n alternativas possíveis para uma situação qualquer, e não temos nenhuma informação, experiência ou raciocínio que justifique atribuir probabilidade maior a uma algumas do que outras, é razoável atribuir probabilidade $1/n$ a cada alternativa. Neste caso dizemos que essas alternativas tem uma *distribuição uniforme* de probabilidade.

Um exemplo de distribuição uniforme é o sorteio de um item entre n outros. Para que o sorteio seja justo é importante que ele seja feito de modo que cada item tenha a mesma probabilidade de ser escolhido. Neste caso dizemos que a escolha é *perfeitamente aleatória*. Esse conceito é importante em muitos jogos ‘de azar’, como cara-ou-coroa, palitinho, par-ou-ímpar, dados, roletas, baralhos, etc.. Esses jogos dependem de dispositivos ou ações que podem dar dois ou mais resultados distintos. Para que o jogo seja justo, é essencial que os jogadores não tenham nenhum conhecimento prévio sobre o resultado, de modo que todos atribuam uma distribuição uniforme de probabilidade ao mesmo.

Por outro lado, é importante observar que a teoria não diz como atribuir as probabilidades de afirmações elementares, mas apenas como combiná-las para obter as probabilidades de afirmações compostas. É importante notar que as probabilidades dependem do observador: se um jogador troca o dado “honesto” por um viciado, ele pode (e deve) atribuir probabilidades diferentes a cada número.

13.1.2 Princípio da exclusão mútua

Intuitivamente, parece pouco razoável termos confiança ao mesmo tempo em duas afirmações contraditórias. Na teoria da probabilidade, essa intuição é formalizada pelo *princípio da exclusão mútua*, ou *aditividade*: se duas proposições P e Q não podem ser verdadeiras ao mesmo tempo (isto é, $P \rightarrow \neg Q$ e $Q \rightarrow \neg P$), então devemos ter $\Pr(P) + \Pr(Q) \leq 1$.

Por exemplo, considere as afirmações “o Diretor está agora em São Paulo” e “o Diretor está agora no Rio de Janeiro”. Quaisquer que sejam as informações que temos a respeito do paradeiro do Diretor, não faz sentido atribuir probabilidade 0,75 para a primeira e 0,80 para a segunda, pois se uma delas for verdadeira, a outra não é.

Essa regra pode ser generalizada para três ou mais proposições P_1, P_2, \dots, P_n . Essas proposições são *mutuamente exclusivas* se sabemos que $P_i \rightarrow \neg P_j$, para quaisquer i e j entre 1 e n com $i \neq j$. Nesse caso, o princípio da exclusão mútua exige que $\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) \leq 1$.

13.1.3 Princípio da exaustão

Por outro lado, se sabemos que pelo menos uma dentre duas afirmações é verdadeira, não é razoável termos pouca confiança nas duas afirmações. Por exemplo, não é razoável não acreditar nem na afirmação “o lucro será maior que R\$ 10.000” nem na afirmação “o lucro será menor que R\$ 20.000”, pois pelo menos uma dessas afirmações com certeza é verdadeira.

Na teoria da probabilidade, essa regra é formalizada pelo *princípio da exaustão*: se sabemos que $P \vee Q$ é verdadeiro, então devemos ter $\Pr(P) + \Pr(Q) \geq 1$. No exemplo acima, podemos atribuir probabilidade 1/2 ou 3/4 para ambas, mas não 1/4; se atribuirmos probabilidade 0,30 para a primeira, podemos atribuir 0,80 para a segunda, mas não 0,50.

Mais geralmente se sabemos que $P_1 \vee P_2 \vee \dots \vee P_n$ é verdadeiro, então devemos ter $\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) \geq 1$.

13.1.4 Princípio da complementaridade

Juntando o princípio da exclusão e da exaustão, podemos concluir que se uma afirmação P é o oposto lógico (negação) da afirmação Q , então a soma das probabilidades deve ser exatamente 1. Ou seja, para qualquer afirmação P , temos

$$\Pr(P) + \Pr(\neg P) = 1 \quad (13.1)$$

ou seja

$$\Pr(\neg P) = 1 - \Pr(P) \quad (13.2)$$

Por exemplo, se a probabilidade de “vai chover amanhã” é 3/4, a probabilidade de “não vai chover amanhã” tem que ser 1/4. Esta regra é conhecida como o *princípio da complementaridade*.

Esta regra também pode ser generalizada para três ou mais afirmações. Suponha que sabemos que exatamente uma das afirmações P_1, P_2, \dots, P_n é verdadeira. Isto é, sabemos que elas são mutuamente exclusivas, mas também que uma delas tem que ser verdadeira. Então devemos ter

$$\Pr(P_1) + \Pr(P_2) + \dots + \Pr(P_n) = 1 \quad (13.3)$$

Por exemplo, suponha que alguém escolheu e retirou uma carta de um baralho comum. Considere as afirmações “a carta é ouros”, “a carta é copas”, “a carta é paus”, “a carta é espadas”, ou “a carta é um coringa”. Como a carta só pode ser de um tipo, e tem que ser de um desses cinco tipos, então as probabilidades dessas afirmações devem somar 1.

Observe que este princípio é respeitado quando atribuímos probabilidade $1/n$ para n alternativas igualmente prováveis.

13.1.5 Princípio da exclusão e inclusão

Os princípios acima podem ser vistos como corolários de um princípio mais geral: para quaisquer afirmações P e Q , devemos ter

$$\Pr(P \vee Q) = \Pr(P) + \Pr(Q) - \Pr(P \wedge Q) \quad (13.4)$$

Compare este princípio com a fórmula para cardinalidade de conjuntos

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (13.5)$$

Exercício 13.1: Contagens em uma fábrica mostraram que 5% dos parafusos tem um defeito na rosca, 4% tem um defeito na cabeça, e 2% tem um defeito em ambas as partes. Qual é a probabilidade de que um desses parafusos, escolhido ao acaso, tenha algum defeito?

13.1.6 Princípio da independência

Um dado e uma moeda são atirados ao mesmo tempo. Como discutimos acima, é razoável atribuir probabilidade $1/6$ à afirmação “o resultado do dado será 3”, e probabilidade $1/2$ à afirmação “o resultado da moeda será cara”. Que probabilidade devemos atribuir à conjunção dessas duas frases, ou seja “o resultado do dado será 3, e o da moeda será cara”?

Uma maneira de fazer esta escolha é observar que há 12 possíveis resultados para os dois lances. Vamos denotar por $D(x)$ e $M(y)$, respectivamente, os predicados “o resultado do dado será x ”, e “o resultado da moeda será y ”. As 12 possibilidades correspondem às afirmações

$$\begin{aligned} D(1) \wedge M(\text{cara}) & D(1) \wedge M(\text{coroa}) \\ D(2) \wedge M(\text{cara}) & D(2) \wedge M(\text{coroa}) \\ D(3) \wedge M(\text{cara}) & D(3) \wedge M(\text{coroa}) \\ D(4) \wedge M(\text{cara}) & D(4) \wedge M(\text{coroa}) \\ D(5) \wedge M(\text{cara}) & D(5) \wedge M(\text{coroa}) \\ D(6) \wedge M(\text{cara}) & D(6) \wedge M(\text{coroa}) \end{aligned} \quad (13.6)$$

Estas afirmações são mutuamente exclusivas e esgotam todas as possibilidades, e portanto a soma de suas probabilidades deve ser 1. Se não temos nenhuma razão para suspeitar que o dado de alguma maneira influencie a moeda, ou vice-versa, então é razoável atribuir a mesma probabilidade ($1/12$) a estas 12 afirmações.

Note que $1/12$ é o produto de $\Pr(D(x)) = 1/6$ e $\Pr(M(y)) = 1/6$. Temos portanto que $\Pr(D(x) \wedge M(y)) = \Pr(D(x))\Pr(M(y))$ para quaisquer x e y .

Este é um exemplo de uma regra geral, o *princípio da independência*. Por definição, duas afirmações P e Q são ditas *independentes* se e somente se

$$\Pr(P \wedge Q) = \Pr(P) \Pr(Q) \quad (13.7)$$

O princípio da independência diz que, se não sabemos de nenhuma ligação ou influência entre o valor lógico de uma afirmação P e o de outra afirmação Q , então é razoável supor que elas são independentes; ou seja, é razoável atribuir à conjunção $P \wedge Q$ o produto das respectivas probabilidades.

Exercício 13.2: Dois dados, um vermelho e um verde, são atirados ao mesmo tempo. Qual é a probabilidade de que o resultado do dado vermelho seja menor que 4, e o do dado verde seja maior que 1?

Exercício 13.3: Se as afirmações P e Q são independentes, quanto vale $\Pr(P \vee Q)$ em função de $\Pr(P)$ e $\Pr(Q)$?

Exercício 13.4: Contagens em uma fábrica mostraram que 20% dos parafusos tem um defeito na rosca, 30% tem um defeito na cabeça. Supondo que os defeitos afetam as duas partes do parafuso de maneira independente, qual é a probabilidade de que um desses parafusos, escolhido ao acaso, tenha algum defeito?

13.1.7 Relação com a lógica clássica

A teoria da probabilidade inclui a lógica clássica como caso particular. Mais precisamente, atribuir probabilidade 0 a uma afirmação equivale a acreditar que a afirmação é falsa; e atribuir probabilidade 1 equivale a acreditar que ela é verdadeira. Se todas as afirmações tem probabilidade 0 ou 1, as regras e conceitos da lógica clássica podem ser traduzidos por regras e conceitos da probabilidade. Por exemplo, o conetivo $P \rightarrow Q$ equivale a afirmar que $\Pr(Q|P) = 1$.

13.2 Variável aleatória

Uma *variável aleatória* é uma variável (parâmetro, quantia) X cujo valor é conhecido apenas parcialmente, no sentido probabilístico. Isto é, sabemos que o valor de X é algum elemento de um certo conjunto D , o *domínio* da variável; e, para qualquer v em D , temos uma medida de probabilidade $\Pr(X = v)$ para a afirmação “ $X = v$ ”. A função que a cada $v \in D$ associa a probabilidade $\Pr(X = v)$ é chamada de *distribuição de probabilidade* (ou simplesmente *distribuição*) da variável X .

Observe que, se u, v são elementos distintos de D , então as afirmações “ $X = u$ ” e “ $X = v$ ” são mutuamente exclusivas. Além disso, sabemos que existe algum elemento v em D tal que a afirmação “ $X = v$ ” é verdadeira. Pelo princípio de inclusão e exclusão, temos portanto que

$$\sum_{v \in D} \Pr(X = v) = 1$$

Observe também que, nestas condições, temos que atribuir $\Pr(X = v) = 0$ para qualquer valor v que não está no conjunto D .

Exemplo 13.1: Um dado foi lançado, mas o resultado da jogada ainda está oculto. Seja X a variável aleatória cujo valor é esse resultado. Sabemos que o domínio de X é o conjunto $D = \{1, 2, \dots, 6\}$. Como não temos motivos para distinguir entre esses resultados, é razoável atribuir probabilidades iguais ($1/6$) para cada valor em D , e probabilidade zero para qualquer outro valor. Em particular, $\Pr(X = 3) = \Pr(X = 5) = 1/6$, e $\Pr(X = 0) = \Pr(X = 7) = \Pr(X = 1/2) = 0$.

Variáveis aleatórias com valores numéricos podem ser combinadas com operações aritméticas e funções matemáticas, resultando em outras variáveis aleatórias. Por exemplo, se α é um número real, a fórmula $\alpha X + \sqrt{Y}$ denota a variável aleatória cujo valor é $\alpha u + \sqrt{v}$, onde u é o valor de X e v o valor de Y . A distribuição dessa nova variável é determinada pelas distribuições de probabilidades de X e de Y .

Exercício 13.5: Sejam X e Y os resultados obtidos atirando-se dois dados de cores diferentes, cada um com distribuição uniforme de probabilidades. Determine a distribuição das seguintes variáveis derivadas de X e Y :

1. X^2
2. $X \bmod 3$
3. $X + Y$
4. $\min\{X, Y\}$

Neste livro só vamos tratar de variáveis aleatórias cujos domínios são conjuntos discretos (finitos ou enumeráveis). A teoria pode ser estendida para variáveis com domínios não enumeráveis, como os números reais; mas esse assunto merece uma disciplina à parte.

13.3 Valor esperado

Um uso importante (e o mais antigo) da teoria da probabilidade é avaliar o ganho ou perda que pode decorrer de uma escolha ou acontecimento cujo resultado é desconhecido, como por exemplo uma aposta ou um investimento na bolsa.

Suponha por exemplo que atiramos uma moeda e apostamos R\$ 30 contra R\$ 10 que o resultado será cara. Temos igual chance de ganhar R\$ 10 (se sair cara) e perder R\$ 30 (se sair coroa). Ou seja,

$$\Pr(\text{"nosso ganho será R\$ 10"}) = \Pr(\text{"nosso ganho será R\$ - 30"}) = \frac{1}{2}$$

Intuitivamente, se repetirmos essa aposta n vezes, em aproximadamente metade das vezes vamos ganhar 10 e na outra metade perder 30; portanto o ganho por aposta, em média, será aproximadamente

$$\frac{\frac{n}{2}(\text{R\$ } 10) + \frac{n}{2}(\text{R\$ } - 30)}{n} = \text{R\$ } - 10 \quad (13.8)$$

Para entender melhor este exemplo, suponha que repetimos duas vezes essa aposta. Temos quatro possibilidades: perder nas duas vezes, só na primeira, só na segunda, ou ganhar nas duas. Nosso ganho médio por aposta será respectivamente, $(-30 - 30)/2 = -30$, $(-30 + 10)/2 = -10$, $(10 - 30)/2 = -10$, e $(10 + 10)/2 = +10$. Supondo que o resultado de cada lance seja independente

dos anteriores, e denotando por $G(x)$ o predicado “nosso ganho médio por aposta será x ”, teremos então

$$\begin{aligned}\Pr(G(-30)) &= 1/4 \\ \Pr(G(-10)) &= 1/4 + 1/4 = 1/2 \\ \Pr(G(+10)) &= 1/4\end{aligned}\tag{13.9}$$

Ou seja, o ganho médio R\$ -10 é duas vezes mais provável que R\$ -30 ou R\$ $+10$. Para quatro apostas seguidas, podemos ter 0, 1, 2, 3, ou 4 acertos, com ganhos médios por aposta de -30 , -20 , -10 , 0 e $+10$, respectivamente. As probabilidades são

$$\begin{aligned}\Pr(G(-30)) &= \binom{4}{0}/2^4 = 1/16 \\ \Pr(G(-20)) &= \binom{4}{1}/2^4 = 4/16 \\ \Pr(G(-10)) &= \binom{4}{2}/2^4 = 6/16 \\ \Pr(G(0)) &= \binom{4}{3}/2^4 = 4/16 \\ \Pr(G(+10)) &= \binom{4}{4}/2^4 = 1/16\end{aligned}\tag{13.10}$$

Como se pode ver, é muito mais provável que o ganho médio por aposta seja R\$ -10 do que qualquer outro valor. A medida que o número de apostas aumenta, essa tendência permanece: o valor mais provável para o ganho médio por aposta será R\$ -10 .

Em geral, suponha que temos uma variável aleatória X que pode assumir qualquer valor de um conjunto de valores numéricos D . O *valor médio esperado* (ou simplesmente o *valor esperado*) de X é, por definição

$$\mathcal{E}X = \sum_{v \in D} v \Pr(X = v)\tag{13.11}$$

Para entender esta fórmula, suponha que temos uma coleção grande com N variáveis, todas elas semelhantes a X mas tais que o valor de uma delas não tem influência nos valores das outras. Nesse caso, o número de variáveis que tem valor v será aproximadamente $N \Pr(X = v)$.

Observe que se D tem um número finito n valores distintos, e todos os valores de D são igualmente prováveis, então $\Pr(X = v) = 1/n$, e a fórmula do valor esperado (13.11) reduz-se à média aritmética dos elementos de D .

Exercício 13.6: Furar um poço de petróleo em determinada região custa R\$500.000, e tem 30% de chance de encontrar óleo. Se isso acontecer, o poço pode ser vendido por R\$800.000. Caso contrário o investimento é totalmente perdido. Qual o ganho esperado por poço?

Quando o domínio da variável é um conjunto infinito, o valor esperado pode ser infinito, mesmo que todos os seus valores possíveis sejam finitos. Por exemplo, considere a variável X cujo valor é um inteiro positivo, tal que $\Pr(X = k) = (6/\pi^2)/k^2$ para todo $k \in \mathbb{N} \setminus \{0\}$. Esta distribuição de probabilidades é válida, pois verifica-se que a soma de todas as probabilidades é 1. Entretanto, o valor esperado de X deveria ser a somatória

$$\mathcal{E}(X) = \sum_{k=0}^{\infty} k \cdot \frac{A}{k^2} = A \sum_{k=0}^{\infty} \frac{1}{k}$$

que, como sabemos, não tem valor finito (veja seção 8.6).

O valor esperado pode ser definido para qualquer variável cujos valores podem ser somados e multiplicados por um número real. Por exemplo, suponha que o valor de uma variável aleatória X é um par (u, v) , onde u é o resultado de lançar uma moeda ($0 = \text{cara}$, $1 = \text{coroa}$), e v é o resultado de lançar um dado (um inteiro entre 1 e 6); sendo que cada par possível tem a mesma probabilidade $1/12$. Note que esses pares podem ser considerados vetores do espaço \mathbb{R}^2 . Portanto podemos calcular o valor esperado de X

$$\mathcal{E}(X) = \frac{1}{12} ((0, 1) + (0, 2) + \cdots + (1, 5) + (1, 6)) = \left(\frac{1}{6}, \frac{7}{2}\right)$$

13.3.1 Propriedades do valor esperado

Seja X uma variável aleatória com domínio numérico, sejam α e β dois números reais quaisquer. Nesse caso, pode-se provar que

$$\mathcal{E}(\alpha X + \beta) = \alpha \mathcal{E}(X) + \beta \quad (13.12)$$

Porém, se uma variável aleatória Z depende de X de maneira não linear (por exemplo, se Z é o quadrado de X), não existe uma fórmula geral que relacionem $\mathcal{E}(Z)$ a $\mathcal{E}(X)$ (Veja o exercício 13.8.)

Sejam X e Y duas variáveis aleatórias com valores numéricos, e seja Z a variável aleatória, denotada por $X + Y$, cujo valor é a soma dos valores de X e de Y . Verifica-se que

$$\mathcal{E}(Z) = \mathcal{E}(X) + \mathcal{E}(Y) \quad (13.13)$$

Estas fórmulas valem mesmo que as variáveis X e Y tenham alguma dependência entre si. Note que não há fórmulas análogas para outras operações (como produto, divisão, etc.).

Exercício 13.7: Um dado vai ser lançado, e a seguinte aposta é oferecida: o cliente paga R\$7,00 ao banqueiro, e recebe em reais o dobro do valor que sair no dado. Por exemplo, se sair um 4, o cliente recebe R\$8,00, obtendo um ganho líquido de R\$1,00. Qual é o ganho esperado do cliente?

Exercício 13.8: Na mesma situação do exercício 13.7, uma outra aposta é oferecida: cliente paga R\$49,00 ao banqueiro, e recebe em reais o dobro do quadrado do valor que sair no dado. Por exemplo, se sair um 6, o cliente recebe $2 \times 6^2 = \text{R}\$72,00$, obtendo um ganho líquido de R\$23,00. Qual é o ganho esperado do cliente?

13.4 Mediana

O valor esperado de uma variável aleatória X pode em muitos casos ser considerado o “valor típico” de X . Por exemplo, se X é a altura (em metros) de uma pessoa que não vimos ainda, o valor esperado de X para a população brasileira é próximo a 1,70 m. Podemos então imaginar o “brasileiro típico” como tendo essa altura.

Porém este raciocínio nem sempre é apropriado. Por exemplo, suponha uma vila com 99 casas térreas e um prédio de 101 andares, e considere a variável aleatória X que é o número de andares de um edifício arbitrário dessa vila, escolhido com probabilidade uniforme. O valor esperado da

variável X será 2, mas obviamente não é correto dizer que o “edifício típico” dessa vila tem dois andares.

Devido a exemplos como esse, foram propostas outras maneiras de obter o “valor típico” de uma variável aleatória. O mais comum é a *mediana*. Idealmente, este é um valor v tal que $\Pr(X \leq v) \geq 1/2$ e $\Pr(X \geq v) \geq 1/2$.

Por exemplo, suponha que a variável aleatória X pode ter qualquer valor inteiro entre 1 e 6, com as seguintes probabilidades

k	1	2	3	4	5	6
$\Pr(X = k)$	$\frac{6}{20}$	$\frac{2}{20}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{7}{20}$	$\frac{1}{20}$

Neste caso podemos tomar a mediana de X como sendo 4, pois

$$\begin{aligned} \Pr(X \leq 4) &= \frac{6}{20} + \frac{2}{20} + \frac{1}{20} + \frac{3}{20} = \frac{12}{20} \geq \frac{1}{2} \\ \Pr(X \geq 4) &= \frac{3}{20} + \frac{7}{20} + \frac{1}{20} = \frac{11}{20} \geq \frac{1}{2} \end{aligned}$$

Note que o valor esperado de X é

$$1 \cdot \frac{6}{20} + 2 \cdot \frac{2}{20} + 3 \cdot \frac{1}{20} + 4 \cdot \frac{3}{20} + 5 \cdot \frac{7}{20} + 6 \cdot \frac{1}{20} = \frac{66}{20} = 3,3$$

Note porém que pode haver diversos valores v que satisfazem a condição $\Pr(X < v) = \Pr(X > v)$. Por exemplo, se a distribuição de probabilidades de X for

k	1	2	3	4	5	6
$\Pr(X = k)$	$\frac{6}{20}$	$\frac{2}{20}$	$\frac{2}{20}$	$\frac{1}{20}$	$\frac{8}{20}$	$\frac{1}{20}$

então, para qualquer valor v tal que $3 < v < 4$, teremos $\Pr(X \leq v) = (6 + 2 + 2)/20 = 1/2$ e $\Pr(X \geq v) = (1 + 8 + 1)/20 = 1/2$.

Quando isso acontece, pode-se provar que os valores de v que satisfazem a definição formam um intervalo finito dos números reais. Nesses casos, alguns autores definem a mediana como sendo o ponto médio desse intervalo; no exemplo acima, seria $v = (3 + 4)/2 = 3,5$.

Exercício 13.9: Seja X o quadrado de um número entre 1 e 6 que será obtido pelo lançamento de um dado. Note que o valor de X pode ser 1, 4, 9, 16, 25, ou 36. Qual é o valor esperado da variável X ? E sua mediana?

Exercício 13.10: Seja X o *produto* dos dois números entre 1 e 6 que serão obtidos pelo lançamento de dois dados. Qual é a distribuição de probabilidades da variável X ? Qual é seu valor esperado? E sua mediana?

Exercício 13.11: Prove que qualquer variável aleatória com valores inteiros tem uma mediana.

13.5 Moda

Outra maneira de definir o “valor típico” de uma variável aleatória é tomar o *valor mais provável*, também chamado de *moda* da variável. Por exemplo, se a distribuição for

k	1	2	3	4	5	6
$\Pr(X = k)$	$\frac{6}{20}$	$\frac{2}{20}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{7}{20}$	$\frac{1}{20}$

diremos que a moda de X é 5. Por outro lado, se as probabilidades forem um pouco diferentes

k	1	2	3	4	5	6
$\Pr(X = k)$	$\frac{7}{20}$	$\frac{2}{20}$	$\frac{1}{20}$	$\frac{3}{20}$	$\frac{6}{20}$	$\frac{1}{20}$

A moda será 1.

13.6 Variância e desvio padrão

Em muitas situações, não basta saber o valor esperado $\mathcal{E}(X)$ de uma variável aleatória; é preciso também saber até que ponto o valor da variável pode diferir desse valor esperado.

Considere por exemplo as variáveis aleatórias X e Y , que podem assumir valores entre 1 e 5 com as seguintes probabilidades:

k	1	2	3	4	5
$\Pr(X = k)$	$\frac{1}{20}$	$\frac{7}{20}$	$\frac{4}{20}$	$\frac{7}{20}$	$\frac{1}{20}$
$\Pr(Y = k)$	$\frac{7}{20}$	$\frac{2}{20}$	$\frac{2}{20}$	$\frac{2}{20}$	$\frac{7}{20}$

As duas variáveis tem o mesmo valor esperado $v = 3$, mas intuitivamente podemos ver que Y varia mais do que X . Como podemos transformar essa intuição em números?

A maneira mais comum é calcular a *variância* $\mathcal{V}(X)$ da variável, definida pela fórmula

$$\mathcal{V}(X) = \sum_{v \in D} (v - \mathcal{E}(X))^2 \Pr(X = v) \quad (13.14)$$

Pode-se verificar que este é o valor esperado da variável $Y = (X - \mathcal{E}(X))^2$.

No exemplo acima, temos

$$\begin{aligned} \mathcal{V}(X) &= (1 - 3)^2 \cdot \frac{1}{20} + (2 - 3)^2 \cdot \frac{7}{20} + (3 - 3)^2 \cdot \frac{4}{20} + (4 - 3)^2 \cdot \frac{7}{20} + (5 - 3)^2 \cdot \frac{1}{20} = \frac{26}{20} = 1,3 \\ \mathcal{V}(Y) &= (1 - 3)^2 \cdot \frac{7}{20} + (2 - 3)^2 \cdot \frac{2}{20} + (3 - 3)^2 \cdot \frac{2}{20} + (4 - 3)^2 \cdot \frac{2}{20} + (5 - 3)^2 \cdot \frac{7}{20} = \frac{60}{20} = 3,0 \end{aligned}$$

evidenciando assim que os valores de Y tendem a estar mais longe de sua média do que os valores de X .

Observe que as parcelas $(v - \mathcal{E}(X))^2$ da somatória (13.14) nunca são negativas, portanto a variância também não pode ser negativa. Além disso, a variância só pode ser zero se todas as parcelas forem zero, ou seja se a variável X só pode ter um valor — que é portanto seu valor esperado $\mathcal{E}(X)$. Se ela pode assumir dois ou mais valores distintos, com probabilidades diferentes de zero, então a variância será estritamente positiva.

Observe que, se o domínio D da variável X é um conjunto infinito, a variância pode ser infinita (mesmo que o valor esperado exista e seja finito). Por exemplo, seja $D = \mathbb{Z} \setminus \{0\}$, e $\Pr(X = v) = B/|v|^3$, onde B é uma constante tal que a soma das probabilidades seja 1. O valor esperado existe ($\mathcal{E}(X) = 0$). Porém, temos

$$\sum_{v \in D} \Pr(X = v)(v - \mathcal{E}(X))^2 = 2 \sum_{k=1}^{+\infty} k = 1^{+\infty} \frac{B}{v^3} v^1 = 2B \sum_{k=1}^{+\infty} k = 1^{+\infty} \frac{1}{v}$$

que, como sabemos, é infinita.

13.6.1 Propriedades da variância

Seja X uma variável aleatória com valores numéricos. Sejam α e β dois valores reais arbitrários. Verifica-se então que

$$\mathcal{V}(\alpha X + \beta) = \alpha^2 \mathcal{V}(X) \quad (13.15)$$

Note que somar uma constante β a uma variável não altera sua variância.

Se X e Y são duas variáveis aleatórias *independentes*, verifica-se que

$$\mathcal{V}(X + Y) = \mathcal{V}(X) + \mathcal{V}(Y) \quad (13.16)$$

Esta fórmula não vale se soubermos de alguma dependência entre as variáveis X e Y (isto é, se atribuirmos a alguma afirmação do tipo “ $(x = u) \wedge (Y = v)$ ” uma probabilidade diferente de $\Pr(X = u)\Pr(Y = v)$). Nesse caso, a variância de $X + Y$ pode ser maior ou menor que $\mathcal{V}(X) + \mathcal{V}(Y)$.

13.6.2 Desvio padrão

Pode-se dizer que, quanto maior a variância, mais “espalhada” é a distribuição de probabilidade da variável. Entretanto, não é fácil interpretar o valor numérico da variância. Por exemplo, se o valor de X é uma medida em metros, a variância é medida em metros quadrados. Uma medida de “espalhamento” que é mais fácil de interpretar é o *desvio padrão*, definido como a raiz quadrada da variância:

$$\mathcal{D}(X) = \sqrt{\mathcal{V}(X)} = \sqrt{\sum_{v \in D} (v - \mathcal{E}(X))^2 \Pr(X = v)}$$

O desvio padrão é medido com as mesmas unidades da variável. Informalmente, pode ser interpretado como o valor “típico” da diferença entre o valor da variável e seu valor esperado.

Exemplo 13.2: Suponha um lote de parafusos que deveriam ser todos iguais, e Seja X o comprimento real de um desses parafusos, escolhido ao acaso. Se dissermos que o valor esperado de X é 150 mm e o desvio padrão é 1 mm, estamos dizendo que o comprimento do parafuso dificilmente será muito maior que 151 mm ou muito menor que 149 mm.

Esta interpretação informal do desvio padrão tem por base o seguinte resultado, devido ao matemático russo Pafnuti Chebyshev ou Tchebychev (1821–1894):

Teorema 13.1: Para qualquer variável aleatória X , e qualquer número real $\alpha \geq 1$,

$$\Pr(|X - \mathcal{E}(X)| \geq \alpha \mathcal{D}(X)) \leq \frac{1}{\alpha^2} \quad (13.17)$$

A demonstração deste resultado foge do escopo deste livro. Em outras palavras, se $\mathcal{E}(X) = \mu$ e $\mathcal{D}(X) = \sigma$, então o valor de X estará dentro do intervalo $[\mu - \alpha\sigma, \mu + \alpha\sigma]$ com probabilidade $1 - 1/\alpha^2$. Para a variável X do exemplo 13.2, o teorema de Tchebychev diz que o comprimento do parafuso (em milímetros) está

- no intervalo $[150 - 2 \cdot 1, 150 + 2 \cdot 1] = [148, 152]$ com probabilidade maior ou igual a $1 - 1/2^2 = 75\%$;

- no intervalo $[150 - 3 \cdot 1, 150 + 3 \cdot 1] = [147, 153]$ com probabilidade maior ou igual a $1 - 1/3^2 \approx 88\%$;
- no intervalo $[150 - 4 \cdot 1, 150 + 4 \cdot 1] = [146, 154]$ com probabilidade maior ou igual a $1 - 1/4^2 \approx 93\%$;

e assim por diante.

Observe que o resultado de Tchebychev vale qualquer que seja a distribuição de probabilidade da variável X .

Exercício 13.12: Seja X uma variável aleatória que pode assumir qualquer valor entre 0 e 100, com igual probabilidade. Calcule o valor esperado, a variância e o desvio padrão de X . Calcule a probabilidade de X estar entre 40 e 60 (inclusive ambos). Compare esse resultado com a probabilidade obtida pelo teorema de Tchebychev.

13.6.3 Covariância

Se X e Y são variáveis aleatórias numéricas, a *covariância* entre as duas é definida pela fórmula

$$C(X, Y) = \sum_{u,v} \Pr((X = u) \wedge (Y = v))(u - \mathcal{E}(X))(v - \mathcal{E}(Y))$$

A covariância é uma medida da dependência entre X e Y . A grosso modo, ela tende a ser positiva quando é muito provável que os valores de X e Y sejam ambos maiores ou ambos menores que suas médias (caso em que o produto $(u - \mathcal{E}(X))(v - \mathcal{E}(Y))$ é positivo). Ela tende a ser negativa quando X e Y tendem a variar em direções opostas em relação a suas médias — quando um está acima da média, o outro provavelmente está abaixo. Observe que $\mathcal{V}(X)$ é a mesma coisa que $C(X, X)$.

É fácil provar que, se X e Y são independentes, então sua covariância é zero. Prova-se também que, para quaisquer variáveis aleatórias numéricas X e Y ,

$$\mathcal{V}(X + Y) = \mathcal{V}(X) + \mathcal{V}(Y) + 2C(X, Y)$$

Note que esta fórmula implica na fórmula (13.16) quando X e Y são independentes.

Exercício 13.13: Encontre duas variáveis aleatórias X e Y que possuem covariância nula mas *não* são independentes.

13.6.4 Coeficiente de correlação

O sinal de $C(X, Y)$ revela o sentido geral da dependência entre X e Y , mas seu valor numérico é difícil de interpretar. Por essa razão é interessante definir o *coeficiente de correlação*

$$\kappa(X, Y) = \frac{C(X, Y)}{\sqrt{\mathcal{V}(X)\mathcal{V}(Y)}} = \frac{C(X, Y)}{\mathcal{D}(X)\mathcal{D}(Y)}$$

Prova-se que este número está sempre entre -1 e $+1$. Ele é zero se X e Y são independentes, $+1$ se cada variável é função linear crescente da outra (isto é, se $Y = \alpha X + \beta$ com $\alpha > 0$) e -1 se cada variável é função linear decrescente da outra ($Y = \alpha X + \beta$ com $\alpha < 0$). Um valor intermediário, por exemplo 0,50, significa que o valor de cada variável é parcialmente função da outra, mas inclui um termo que não depende dela. Neste caso diz-se que *há correlação entre X e Y (positiva ou negativa, conforme o sinal do coeficiente)*.

13.7 Probabilidade condicional

Seja X a variável aleatória cujo valor é o resultado do lançando um dado, e considere as duas afirmações “ X é par” e “ X é ímpar”. Se não temos nenhuma outra informação sobre X , como vimos, é razoável atribuir a probabilidade $1/6$ a cada um dos possíveis valores $1, 2, \dots, 6$, e portanto

$$\begin{aligned}\Pr(X \text{ é par}) &= \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 6) = 1/2 \\ \Pr(X \text{ é ímpar}) &= \Pr(X = 1) + \Pr(X = 3) + \Pr(X = 5) = 1/2\end{aligned}$$

Suponha agora que sabemos que o valor de X não é 3. Que probabilidade devemos atribuir a essas duas afirmações? Não podemos simplesmente eliminar o termo $\Pr(X = 3)$ na segunda fórmula, pois a soma não seria 1. Como a probabilidade do valor ser 3 é zero, temos que corrigir a probabilidade dos demais valores para que elas tenham soma 1. Ou seja, temos que supor $\Pr(X = 3) = 0$ e $\Pr(X = v) = 1/5$ para os demais valores. Então teremos

$$\begin{aligned}\Pr(X \text{ é par}) &= \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 6) = 3/5 \\ \Pr(X \text{ é ímpar}) &= \Pr(X = 1) + \Pr(X = 5) = 2/5\end{aligned}$$

Observe que a informação adicional “ $X \neq 3$ ” afetou não apenas a probabilidade de X ser ímpar, mas também a probabilidade de ele ser par.

Em casos como este, costuma-se usar a notação $\Pr(P|Q)$ para denotar a *probabilidade condicional* da afirmação P , sabendo-se que (ou dado que) a afirmação Q é verdadeira. Verifica-se que essa probabilidade pode ser calculada pela fórmula

$$\Pr(P|Q) = \frac{\Pr(P \wedge Q)}{\Pr(Q)} \quad (13.18)$$

Aplicando esta fórmula ao exemplo acima, a afirmação P seria “ X é ímpar” e Q a afirmação “ $X \neq 3$ ”. Temos então que

$$\begin{aligned}\Pr(P \wedge Q) &= \Pr(X = 1) + \Pr(X = 5) &= 2/6 \\ \Pr(Q) &= \Pr(X = 1) + \Pr(X = 2) + \Pr(X = 4) + \Pr(X = 5) + \Pr(X = 6) &= 5/6 \\ \Pr(P|Q) &= \frac{2/6}{5/6} &= 2/5\end{aligned}$$

Exercício 13.14: Seja X o valor obtido lançando um dado. Calcule, pela fórmula (13.18)

1. $\Pr(X \text{ é par} | X \neq 3)$
2. $\Pr(X \text{ é par} | X \text{ é quadrado perfeito})$
3. $\Pr(X \text{ é primo} | X \text{ é maior que } 2)$

Exercício 13.15: Seja X a soma dos valores obtidos no lançamento de dois dados. Calcule, pela fórmula (13.18)

1. $\Pr(X \text{ é par} | \text{os dois dados deram o mesmo resultado})$
2. $\Pr(X \text{ é par} | \text{os dois dados deram resultados diferentes})$
3. $\Pr(X = 6 | \text{os dois valores não são primos entre si})$

A fórmula da probabilidade condicional é também muito usada na forma inversa:

$$\Pr(P \wedge Q) = \frac{\Pr(P|Q)}{\Pr(Q)} \quad (13.19)$$

Ou seja, uma vez definida a probabilidade de P dado Q , e também a probabilidade de Q , a probabilidade da afirmação “ P e Q ” é simplesmente o produto das duas.

Exercício 13.16: Suponha que a probabilidade de algum hacker tentar violar seu computador no próximo minuto é 10%, e que a probabilidade de tal tentativa ter sucesso é 80%. Qual é a probabilidade de seu computador ser violado por algum hacker no próximo minuto? (Ignore a possibilidade de haver mais de um ataque por minuto.)

Exercício 13.17: Suponha que atiramos dois dados, um verde e um vermelho. Qual a probabilidade de que o dado verde mostre o valor 2, e o dado vermelho mostre o valor 3? E qual é a probabilidade de que um deles mostre o valor 2, e o outro 3? Agora suponha que os dois dados são idênticos, a tal ponto que não podemos dizer qual é um e qual é o outro. Qual é a probabilidade de que um deles mostre 2, e o outro 3?

13.8 Inferência bayesiana

Combinando as fórmulas (13.18) e (13.19), obtemos a equação

$$\Pr(P|Q) = \frac{\Pr(Q|P) \Pr(P)}{\Pr(Q)} \quad (13.20)$$

Esta fórmula é conhecida como *regra de Bayes* ou *teorema de Bayes*, desenvolvida pelo matemático inglês Thomas Bayes ($\approx 1702-1761$) e, independentemente, pelo matemático francês Pierre-Simon Laplace (1749–1827). Ela é geralmente usada quando se quer obter a probabilidade $\Pr(P|Q)$ de uma possível causa P , sabendo-se que uma consequência Q ocorreu, a partir da probabilidade condicional inversa $\Pr(Q|P)$ (de que essa consequência produza essa causa). Este raciocínio probabilístico é conhecido como *inferência bayesiana* ou *dedução bayesiana*.

Por exemplo, considere uma coleção de caixas quadradas e redondas, cada uma contendo uma bola que pode ser azul ou branca. Suponha que há igual número de caixas de cada formato, sendo que há bolas azuis em metade das caixas quadradas, mas em apenas 10% das caixas redondas. Imagine que alguém escolheu uma caixa ao acaso, e encontrou nela uma bola azul. Qual a probabilidade de que ele tenha escolhido uma caixa quadrada? E se a bola for branca?

Se não tivéssemos a informação sobre a bola, seria razoável supor que a caixa era quadrada com probabilidade $1/2$. Porém, como bolas brancas são mais comuns nas caixas redondas, intuitivamente, a informação de que a bola era branca aumenta a probabilidade de que a caixa seja redonda.

Para calcular essas probabilidades, vamos denotar por Q , R , A e B as afirmações “a caixa era quadrada”, “a caixa era redonda”, “a bola era azul” e “a bola era branca”, respectivamente. Pelo

enunciado do problema, temos

$$\begin{aligned} \Pr(Q) &= \frac{1}{2} & \Pr(R) &= \frac{1}{2} \\ \Pr(A|Q) &= \frac{1}{2} & \Pr(B|Q) &= \frac{1}{2} \\ \Pr(A|R) &= \frac{1}{10} & \Pr(B|R) &= \frac{9}{10} \end{aligned}$$

O que se pede são as probabilidades condicionais $\Pr(Q|A)$ e $\Pr(Q|B)$. Para aplicar a fórmula (13.18), precisamos determinar $\Pr(B)$ e $\Pr(Q \wedge B)$. Para chegar lá, temos que calcular as probabilidades de todas as combinações válidas dessas afirmações. Aplicando a fórmula (13.19) temos

$$\begin{aligned} \Pr(Q \wedge A) &= \Pr(A \wedge Q) = \Pr(A|Q) \Pr(Q) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \\ \Pr(Q \wedge B) &= \Pr(B \wedge Q) = \Pr(B|Q) \Pr(Q) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \\ \Pr(R \wedge A) &= \Pr(A \wedge R) = \Pr(A|R) \Pr(R) = \frac{9}{10} \cdot \frac{1}{2} = \frac{9}{20} \\ \Pr(R \wedge B) &= \Pr(B \wedge R) = \Pr(B|R) \Pr(R) = \frac{1}{10} \cdot \frac{1}{2} = \frac{1}{20} \end{aligned}$$

Daí tiramos

$$\begin{aligned} \Pr(A) &= \Pr(B \wedge Q) + \Pr(B \wedge R) = \frac{1}{4} + \frac{1}{20} = \frac{3}{10} \\ \Pr(B) &= \Pr(A \wedge Q) + \Pr(A \wedge R) = \frac{1}{4} + \frac{9}{20} = \frac{7}{10} \end{aligned}$$

portanto

$$\begin{aligned} \Pr(Q|A) &= \frac{\Pr(Q \wedge A)}{\Pr(A)} = \frac{\Pr(A|Q) \Pr(Q)}{\Pr(A)} = \frac{1/4}{3/10} = \frac{5}{6} \approx 0,833 \\ \Pr(Q|B) &= \frac{\Pr(Q \wedge B)}{\Pr(B)} = \frac{\Pr(B|Q) \Pr(Q)}{\Pr(B)} = \frac{1/4}{7/10} = \frac{5}{14} \approx 0,357 \end{aligned}$$

Observe que a informação adicional “a bola sorteada é azul” aumenta a probabilidade de que a caixa escolhida seja quadrada, de 0,5 a 0,833

Generalizando este exemplo, suponha que temos m afirmações A_1, A_2, \dots, A_m , os *antecedentes*, exaustivas e mutuamente exclusivas, cujo valor lógico pode influir na probabilidade de outras n afirmações B_1, B_2, \dots, B_n , os *consequentes*, também exaustivas e mutuamente exclusivas. As afirmações A_i podem ser as alternativas possíveis para um evento-causa (no exemplo acima, a escolha caixa, quadrada ou redonda), e as afirmações B_j as possíveis consequências do mesmo (a cor da bola). Suponha que atribuímos probabilidades $\Pr(A_i)$ para cada antecedente A_i , sem levar em conta as afirmações B_j ; e temos também a probabilidade condicional $\Pr(B_j|A_i)$ de cada consequente, dado o antecedente. Uma vez sabido que um determinado B_j é verdadeiro, a probabilidade de cada A_i passa a ser

$$\Pr(A_i|B_j) = \frac{\Pr(A_i \wedge B_j)}{\Pr(B_j)} = \frac{\Pr(A_i \wedge B_j)}{\sum_{k=1}^m \Pr(B_j \wedge A_k)} = \frac{\Pr(B_j|A_i) \Pr(A_i)}{\sum_{k=1}^m \Pr(B_j|A_k) \Pr(A_k)} \quad (13.21)$$

Note que para aplicar a fórmula (13.21) precisamos atribuir uma probabilidade $\Pr(A_i)$ a cada antecedente, independente de qual consequente é verdadeiro. O fator $\Pr(A_i)$ nesta fórmula é chamado de *probabilidade a priori* do antecedente A_i , enquanto que o resultado $\Pr(A_i|B_j)$ é sua *probabilidade a posteriori*.

A influência das probabilidades *a priori* $\Pr(A_i)$ é uma característica essencial da inferência bayesiana. Elas podem ser vistas como “preconceitos” que temos a respeito das afirmações A_i , antes de olharmos para as evidências B_j . A fórmula portanto explicita quantitativamente a constatação comum, de que nossos preconceitos sempre afetam nossa interpretação dos fatos.

Exercício 13.18: Suponha que há duas gavetas em uma mesa de jogo. Uma delas contém um dado “honesto”, que dá cada valor de 1 a 6 com igual probabilidade $1/6$; a outra contém um dado “viciado”, que dá o valor 6 com probabilidade $1/2$, e os valores de 1 a 5 com probabilidade $1/10$ cada.

1. Uma pessoa escolhe (sem você ver) um desses dois dados. Na falta de informações, você atribui a probabilidade *a priori* $1/2$ de que esse dado seja viciado. O dado é então lançado e o resultado é 6. Como fica a probabilidade de que o dado seja viciado?
2. Suponha agora que a pessoa seja um notório vigarista, de modo que, mesmo antes de lançar, você dá 90% de chance de que ele tenha escolhido o dado viciado. Como fica essa probabilidade depois que o dado foi lançado, com resultado 6?
3. Finalmente suponha que você confia na pessoa e portanto acredita que ela escolheu o dado honesto, com 90% de probabilidade. Como fica sua confiança nessa hipótese depois que o dado deu 6?

Exercício 13.19: Uma moeda é lançada 10 vezes seguidas, e o resultado é sempre cara. Talvez a moeda seja normal, e esse resultado seja coincidência; ou talvez ela seja uma moeda anormal, com cara dos dois lados. Suponha que a probabilidade *a priori* da moeda ser anormal é p . Qual é a probabilidade *a posteriori*, depois desses 10 lances? Faça um gráfico dessa probabilidade em função de p .

13.9 Teoria da informação

Hoje em dia todos conhecem o conceito de *bit* e outras unidades derivadas, como *byte* (8 bits), *megabyte* (10^6 ou 2^{20} bytes, conforme o contexto), *gigabyte* (10^9 ou 2^{30} bytes) etc. Em geral esses conceitos são usados para descrever tamanhos de arquivos, capacidade de memória, taxas de transmissão, etc. Porém é necessário distinguir entre a *capacidade de armazenamento de informação* de tais sistemas, e a *quantidade de informação* contida neles em determinado momento. Este segundo conceito é o centro da *teoria da informação*, desenvolvida principalmente em meados do século 20 pelo matemático e engenheiro americano Claude Shannon (1916–2001).

13.9.1 Capacidade de informação

Considere um sistema físico (real ou imaginário) que em qualquer momento pode assumir um único estado dentre uma coleção finita de estados possíveis; sendo que esse estado pode ser identificado com precisão por algum tipo de teste ou medida. Por exemplo, uma moeda sobre uma mesa, que pode estar na posição ‘cara’ ou ‘coroa’; um dado de jogar, que pode estar virado com qualquer face para cima, de 1 a 6; uma chave elétrica, que pode estar ‘desligada’ ou ‘ligada’; um fio elétrico, que pode estar a zero volts ou a +5 volts; uma barra de ferro, que pode estar magnetizada em dois sentidos diferentes; e assim por diante. Tal objeto é dito um *sistema discreto*.

Suponha que o sistema tem apenas dois estados possíveis (ou seja, é um *sistema binário*). Por definição, a capacidade de informação de tal sistema é 1 bit. Se o sistema tem 2^b estados possíveis, sua capacidade é b bits. Observe que podemos numerar os estados de tal sistema em base 2 usando

b algarismos, cada qual 0 ou 1: — $0 \cdots 00 = 0$, $0 \cdots 01 = 1$, $0 \cdots 10 = 2$, $0 \cdots 11 = 3$, ..., $1 \cdots 11 = 2^b - 1$. Daí o nome “bit”, que é abreviação do inglês *binary digit*.

Mais geralmente, se o número de estados possíveis n , a capacidade de informação é definida como $\log_2 n = (\ln n)/(\ln 2)$, o logaritmo de n na base 2. Assim, por exemplo, a capacidade de informação de um dado de jogar, em repouso sobre a mesa, é $\log_2 6 = 2,5849625007 \dots$ bits. Note que, se n não é uma potência de 2, a capacidade em bits não é um número inteiro (e, na verdade, é um número irracional). Note também que se o sistema tem apenas um estado possível, sua capacidade de armazenar informação é (como se pode esperar) zero bits.

Esta definição implica na seguinte propriedade:

Teorema 13.2: Se um sistema S consiste de dois sub-sistemas discretos A e B independentes (no sentido de que cada estado possível de A pode co-existir com qualquer estado possível de B , e vice-versa), então a capacidade de S é a soma das capacidades de A e de B .

Exercício 13.20: Determine a capacidade de informação dos seguintes sistemas:

1. Um odômetro (mostrador de quilometragem) de automóvel com 6 algarismos decimais.
2. Um dado em forma de octaedro, com faces numeradas de 1 a 8, em repouso sobre a mesa.
3. Uma cadeia de DNA com 100 elementos (*nucleotídeos*), cada qual podendo ter quatro estruturas químicas possíveis — adenosina (A), timina (T), guanina (G), ou citosina (C).

Exercício 13.21: Determine a capacidade de informação dos seguintes sistemas, constituídos de 4 moedas, cada qual podendo ser de 5, 10, 25, ou 50 centavos, que somente podem ser distinguidas pelo seu valor:

1. Uma pilha, em qualquer ordem.
2. Uma pilha, em ordem crescente de valor.
3. Uma coleção em um saco.
4. Uma pilha onde todas as moedas tem o mesmo valor.

Exercício 13.22: Refaça o exercício 13.21, supondo que todas as moedas de mesmo valor estão marcadas com letras distintas entre ‘A’ e ‘D’. Assim, por exemplo, na alternativa 1, as moedas poderiam ser, na ordem, (10, D), (25, C), (10, B), (10, C) mas não poderiam ser (10, D), (25, C), (10, B), (10, D).

Exercício 13.23: Qual é a capacidade de informação de uma carta retirada de um baralho com 13 cartas? E de um baralho com 52 cartas? Se acrescentarmos um coringa ao baralho, de quanto aumenta a capacidade, em cada caso?

13.9.2 Quantidade de informação

A capacidade de informação de um sistema discreto diz apenas o limite máximo de informação que pode ser armazenada nele. Porém, dependendo de como o sistema é usado, nem toda a capacidade pode ser utilizada.

Por exemplo, considere uma lâmpada que, ao meio-dia, pode estar acesa ou apagada conforme o sol tenha nascido ou não naquele dia. Embora a capacidade de informação desse sistema seja 1 bit, intuitivamente a notícia de que essa lâmpada está acesa não traz muita informação. Por outro lado, uma lâmpada que indica se está chovendo ou não fora do prédio parece fornecer mais informação — muito embora sua *capacidade* de informação seja exatamente a mesma.

A diferença estes dois exemplos está na probabilidade que atribuímos aos dois estados do sistema. No primeiro caso, é natural atribuir probabilidade bem próxima a 1 à afirmação “a lâmpada está acesa”. (A menos que sejamos extremamente pessimistas!) Por isso, a notícia de que essa informação é verdadeira não muda muito nosso estado de conhecimento. Já, no segundo exemplo, faz sentido atribuir probabilidade bem menor que 1 a essa afirmação. (A menos que estejamos na Bolívia, onde nunca chove!)

Para tornar esta intuição mais precisa, suponha que X é uma variável aleatória que pode assumir um certo valor v . A *quantidade de informação* trazida pela notícia “o valor de X é v ” é, por definição,

$$Q(X = v) = \log_2 \frac{1}{\Pr(X = v)} = -\log_2 \Pr(X = v)$$

Este valor, como a capacidade de informação, é medido em bits, e nunca é negativo. Em particular, se X pode assumir n valores distintos com igual probabilidade $\Pr(X = v) = 1/n$, a quantidade de informação que recebemos quando ficamos sabendo o valor de X (qualquer valor de X) é exatamente $Q(X = v) = \log_2 n$ bits — ou seja, a capacidade da variável X .

Porém, se as probabilidades dos valores de X não são iguais, a quantidade de informação pode ser menor ou maior, dependendo do valor. Por exemplo:

Exemplo 13.3: Suponha que um dado está para ser lançado, e X é uma variável que vale 100 se o resultado do dado é 1, e 200 caso contrário. Então as notícias “ $X = 100$ ” e “ $X = 200$ ” carregam as seguintes quantidades de informação:

$$\begin{aligned} Q(X = 100) &= -\log_2 \Pr(X = 100) = -\log_2 \frac{1}{6} \approx 2,5849625 \dots \\ Q(X = 200) &= -\log_2 \Pr(X = 200) = -\log_2 \frac{5}{6} \approx 0,2630344 \dots \end{aligned}$$

Neste exemplo, observe que a notícia “ $X = 200$ ” traz muito menos informação do que a notícia “ $X = 100$ ”, porque tem probabilidade maior — $5/6$ em vez de $1/6$.

13.9.3 Quantidade esperada de informação

No exemplo 13.3, observe também que a notícia “ $X = 100$ ” traz mais que 1 bit de informação — muito embora a variável X tenha apenas dois valores possíveis, e portanto tenha apenas 1 bit de capacidade.

Este paradoxo é resolvido se considerarmos a *quantidade esperada de informação*, ou *entropia*, da variável X . Ou seja, a quantia

$$\mathcal{H}(X) = \sum_v \Pr(X = v) Q(X = v) = \sum_v -\Pr(X = v) \log_2 \Pr(X = v) \quad (13.22)$$

Nesta fórmula, o índice v do somatório assume todos os valores possíveis da variável X . Observe que, como na fórmula (13.11), cada termo desta soma é a quantidade de informação trazida pela notícia “ $X = v$ ”, vezes a probabilidade de recebermos essa notícia. Pode-se verificar que $\mathcal{H}(X)$, assim como cada termo $Q(X = v)$, é um valor real não negativo.

No exemplo 13.3, a quantidade esperada de informação que recebemos ao conhecer o valor de X é

$$\begin{aligned} \mathcal{H}(X) &= \Pr(X = 100) Q(X = 100) + \Pr(X = 200) Q(X = 200) \\ &= \frac{1}{6} \log_2 \frac{6}{1} + \frac{5}{6} \log_2 \frac{6}{5} \\ &\approx \frac{1}{6} 2,5849625 \dots + \frac{5}{6} 0,2630344 \dots \\ &\approx 0,65002241 \dots \end{aligned}$$

Observe que, embora a notícia “ $X = 100$ ” forneça mais de 2,5 bits de informação, ela é muito menos provável que a notícia “ $X = 200$ ”, que fornece menos que 0,27 bits de informação. Assim, a quantidade esperada de informação que ganhamos ao saber o valor de X é cerca de 0,65 bits, ou seja abaixo da capacidade de X (1 bit). Esta última observação é um resultado importante:

Teorema 13.3: Se uma variável aleatória X pode assumir n valores distintos, então a quantidade esperada de informação que ganhamos conhecendo o valor de X é no máximo a capacidade de X , $\log_2 n$; e é exatamente $\log_2 n$ apenas quando todos esses valores podem ocorrer com igual probabilidade $1/n$.

Devido a este teorema, a fórmula (13.22) é muito usada para medir a “uniformidade” da distribuição de probabilidades de uma variável aleatória X . O valor de $\mathcal{H}(X)$ varia entre 0 e $\log_2 n$, onde n é o número de valores possíveis de X . Quanto maior $\mathcal{H}(X)$, mais uniforme a distribuição. Na verdade, a fórmula (13.22) pode ser usada com qualquer lista de n valores reais p_0, p_1, \dots, p_{n-1} não negativos cuja soma é 1.

Observe que se X tem uma distribuição degenerada — com $\Pr(X = v) = 1$ para um único valor v , e zero para os demais valores — então $\mathcal{H}(X)$ é zero. Ou seja, se temos certeza de qual vai ser o valor de X , nossa expectativa é que a revelação desse valor não vai nos trazer nenhuma informação.

Referências Bibliográficas

- [1] Béla Bollobás. *Modern Graph Theory*. Springer, 1998.
- [2] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications*. MacMillan, London, 1976.
- [3] J. A. Bondy and U. S. R. Murty. *Graph Theory*. Springer, 2008.
- [4] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest. *Introduction to Algorithms*. MIT Press, 1989.
- [5] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Matemática Concreta: Fundamentos para Ciência da Computação*. LTC, 1995. Segunda edição.
- [6] Paul R. Halmos. *Teoria Ingênua dos Conjuntos*. Editora da USP, 1960.
- [7] Frank Harary. *Graph Theory*. Addison Wesley, 1972.
- [8] John M. Harris, Jeffrey L. Hirst, and Michael J. Mossinghoff. *Combinatorics and Graph Theory*. Springer, 2000.
- [9] Thomas L. Heath. *The Thirteen Books of Euclid's Elements*. Dover, 1956. Segunda edição.
- [10] David C. Kurtz. *Foundations of Abstract Mathematics*. McGraw-Hill, 1992.
- [11] Luiz Henrique Jacy Monteiro. *Elementos de Álgebra*. Ao Livro Técnico, 1969.
- [12] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 2003. Quinta edição.
- [13] J. Plínio O. Santos, Margarida P. Mello, and Idani T. C. Murari. *Introdução à Análise Combinatória*. Editora da UNICAMP, 1995.
- [14] Daniel J. Velleman. *How to Prove It: A Structured Approach*. Cambridge University Press, 2006. Segunda edição.

Índice Remissivo

- pi
 - algarismos, 27
- n -upla, *veja* ênupla
- água, 192
- álgebra, 17
 - de Boole, 33
- árvore, *veja* grafo árvore
- óctupla, *veja* ênupla
- índice
 - de somatória, *veja* somatória, índice
- ângulo
 - interno, 73
- ênupla, *veja* sequência finita, 122
 - definição, 122
 - elementos, 122
 - igualdade, 122
 - vazia, 122
- absurdo, *veja* prova, implicação por absurdo
- Al-Khowarizmi, 17
- alef (\aleph), *veja* cardinalidade de Cantor
- algarismo, 108, 157
- algoritmo
 - de Euclides, 17
 - demonstração, 15
 - geométrico, 15
- ambiguidade, 28, 29, 33, 56
- amigo, 49
- análise de algoritmos, 17
- antecedente, 30
- Appel, Kenneth, 56
- Appel, Kenneth Ira, 198
- Argentina, 28
- Aristóteles, 15
- arquivo, 101
- arranjo, 152–153
 - contagem, 153
 - de letras, 152
 - definição, 152
 - e permutação, 153
- arroz, 29
- Artur, Rei da Inglaterra, 189
- associatividade, 38
 - da intersecção, 23
 - da união, 23
- auto-referência, *veja* proposição auto-referente
- axioma, 15, 19, 55
 - da aritmética, 70
 - de Euclides, 16
 - do contínuo, 165
- balança, 76, 80
- banana, 48–50
- banco de dados, 167
- bancos de dados, 125
- baralho, 151, 154, 158, 217
- base neperiana (e), 141
- bateria, 33
- Bayes, Thomas, 214
- Bernoulli, Jacob, 75
- Bernstein, Felix, 164
- bijeção, *veja* função bijetora, 161–166
- binômio de Newton, 155
- bipartição, 187
- bit, 106, 216
 - contagem de cadeias, 154
 - definição, 216
- bloco
 - de partição, 25
- boi, 50
- bola, 72, 214
- branco, 30
- Brasília, 28, 30
- Brasil, 27, 28

- byte, 216
- C (linguagem), 120
- cálculo
 - de predicados, 17, 47
 - proposicional, 27–43
- código genético, 217
- círculo, 16
- cadeia, *veja* sequência finita
- caixa, 103, 214
 - jeitos de tampar, 119
 - rotulada, 119
- Cantor, Georg, 19
- Cantor, Georg Ferdinand Ludwig Philipp, 162, 164, 165
- capacidade de armazenamento, *veja* informação, capacidade
- capacidade de informação, *veja* informação, capacidade
- cardinalidade, *veja* conjunto, 161–166
 - comparação, 164
 - contável, 163
 - da união, 156
 - de Cantor (\aleph^k), 165
 - de conjunto finito, 161
 - de conjunto infinito, 161
 - de conjuntos finitos, 164
 - de subconjuntos, 164
 - definição, 161
 - dos inteiros, 162
 - dos números naturais, 163, 165
 - dos números reais, 162–165
 - dos pares de naturais, 162
 - igualdade, 161
 - menor, 164
 - menor ou igual (\leq), 164
- casa, 30
- casas, 29
- cavalo, 77, 192
- celular, 29
- { } (chaves), 19
- Chebyshev, *veja* Tchebychev
- cheque, 32
- circuito
 - digital, 167
 - elétrico, 167
- classe
 - de equivalência, 109–111, 183
 - representante, 110
 - de isomorfismo, 183
- coeficiente binomial, *veja* combinação
 - casos especiais, 154
 - definição, 153
- coeficiente multinomial, *veja* combinação múltipla
- cofre, 191
- Cohen, Paul, 165
- Cole, Frank Nelson, 57
- coloração, *veja* grafo, coloração
- combinação, 153–156
 - algoritmo, 156
 - casos especiais, 154
 - com repetições, *veja* combinação múltipla
 - contagem, 153
 - de letras, 153
 - de respostas em prova, 156
 - definição, 153
 - e arranjo, 153
 - fórmula de Leibniz, 158
 - fórmula de Newton, 155
 - fórmula recursiva, 156
 - identidade de Pascal, 154
 - múltipla, 157–159
 - notação, 153
 - propriedades, 154
 - simetria, 154
 - somatória, 155, 156
 - triângulo de Pascal, 155
- complemento, *veja* conjunto, complemento
- composição
 - de relações, *veja* relação, composição
- comutatividade, 38
 - da intersecção, 23
 - da união, 23
- conclusão, 30
- condição
 - necessária, 31
 - suficiente, 31
- conectivo lógico, *veja* operador lógico
 - em linguagem natural, 28
- conectivo lógico, *veja* operador lógico

- conjectura, *veja* conjetura
- conjetura, 56–57
- aberta, 56
 - das quatro cores, 56
 - de Fermat, 56
 - de Goldbach, 57
 - de Mersenne, 57
 - refutação, 66
 - refutada, 56
- conjunção, *veja* operador conjunção
- conjunto
- cardinalidade, 21, 22, 26, 75, *veja* cardinalidade
 - complemento, 22, 24, 157
 - contável, 163
 - continência, 67
 - de conjuntos, 24
 - de seqüências, 104
 - definição, 19
 - diferença, 25
 - diferença (\setminus), 22
 - diferença simétrica (Δ), 22
 - disjunto, 22, 25
 - dos subconjuntos, *veja* conjunto potência
 - enumerável, 163
 - finito, 21, 161
 - igualdade, 20
 - infinito, 21, 161
 - intersecção, 23–24
 - intersecção (\cap), 22
 - leis de De Morgan, 24
 - notação, 19
 - operação, 21–24, 26
 - ordenado, 101
 - parcialmente, 105
 - totalmente, 104
 - parcialmente ordenado, 105
 - partição, 25, 187
 - por propriedade, 19
 - potência, 22, 75, 101, 109, 164
 - cardinalidade, 25
 - potência ($\mathbb{P}(A)$)
 - definição, 25
 - totalmente ordenado, 104
 - união, 23–24
 - união (\cup), 21
 - universal, 24, 53, 142
 - universal (\mathcal{U}), 22
 - vazio, 21, 24, 63, 94, 142
 - cardinalidade, 21
 - como elemento, 24
 - inclusão, 21
 - partição, 25
 - potência, 25
 - vs. seqüência, 120
- consequência, 30
- consequência lógica, 40
- $\not\supseteq$ (não estr. contém), *veja* inclusão
- $\not\subseteq$ (não contém), *veja* inclusão
- \subseteq (contido), 19
- \supseteq (estr. contém), *veja* inclusão
- \supseteq (contém), *veja* inclusão
- contagem, 151–159
- arranjos, 153
 - cadeias de bits, 154
 - combinações, 153
 - de relações, 87
 - anti-simétrica, 96
 - irreflexivas, 96
 - reflexivas, 96
 - simétrica, 96
 - ordens, 151
 - permutações, 151
 - união, 156
- $\not\subset$ (não estr. contido), *veja* inclusão
- $\not\subseteq$ (não contido), *veja* inclusão
- \subset (estr. contido), *veja* inclusão
- \subseteq (contido), *veja* inclusão
- contra-exemplo, 66, 67
- contradição, 36, 37, 47
- contrapositiva
- de implicação, *veja* proposição contrapositiva
- cor, 77
- cores, 158, *veja* grafo, coloração de faces
- corolário, 55
- correio, 33, 74
- criptografia digital, 17
- cubo, 73, 192
- cubo perfeito, 68

- dado de jogar, 204–206, 208, 213–215, 217, 218
 de equivalência, 62
 De Morgan, *veja* conjunto, leis de
 De Morgan, Augustus, 24, 38, 198
 definição, 55–56
 circular, 20
 contraditória, 20
 definição, 55
 recursiva, 104
 demonstração, 17, 55–68
 por computador, 198
 desarranjo, 119
 desigualdade
 de Bernoulli, 75
 diagonal, 73
 diagonalização, 162–164
 diagrama
 de Hasse, 102–105, 107
 de Venn, 22–24, 26
 dicionário, 104, 106
 diferença, *veja* conjunto, diferença
 de grafos, *veja* grafo, subgrafo, diferença
 \setminus , *veja* conjunto, diferença
 diferença simétrica, *veja* conjunto, diferença simétrica de quantificador, 52
 Δ , *veja* conjunto, diferença simétrica
 dinheiro, 74
 Dirichlet, Johann Peter Gustav Lejeune, 76
 disco, 123
 disjunção, *veja* operador disjunção
 disjunção exclusiva, 46
 operador, *veja* operador disjunção exclusiva
 distributividade, 38
 da intersecção, 23
 da união, 23
 divisibilidade, 59, 67, 68, 168
 divisor, 56, 64
 comum, 17
 definição, 56
 DNA, 217
 dodecaedro, 190, 192
 domínio, *veja* relação, domínio
 de quantificador, 44, 45
 mudança, 50
 omissão, 52
 universal, 53
 domingo, 49
 dualidade lógica, 43

e, *veja* base neperiana
 eleição, 34
 elemento
 definição, 19
 máximo, *veja* máximo
 mínimo, *veja* mínimo
 neutro, 37, 142
 elemento maximal, *veja* maximal
 elemento minimal, *veja* minimal
 encomenda, 32
 entropia, 218, 219
 como medida de uniformidade, 219
 máxima, 219
 nula, 219
 equivalência, 62, *veja* relação de equivalência
 de operadores, 42–43
 lógica, 37–39, 41
 operador, *veja* operador equivalência
 equivalência lógica, 39, 43, 47
 escopo
 esfera, 123
 esgoto, 192
 estado
 de um sistema, *veja* informação, capacidade
 estatística, 17
 estrutura de programa, 167
 estudante, 46, 47, 49
 Euclides, 16, 17, 65
 Euler, Leonhard, 167
 exponencial, 141

 fórmula
 de Bayes, *veja* inferência bayesiana
 de Euler, 194
 de Pólya, 184
 de Tchebychev, *veja* variável aleatória, teorema de Tchebychev
 fórmula de Stirling, 152
 fatorial, 140, 141, 151
 aproximação, 152
 crescimento, 152

- fechadura, 191
 fecho, 100
 - geral, 99
 - reflexivo, 96, 99, 100
 - simétrico, 97, 99, 100
 - transitivo, 97, 99, 100
 feijão, 29
 Fermat, Pierre de, 56
 forma normal
 - conjuntiva, 42
 - disjuntiva, 41–42
 FORTRAN, 120
 Fourier, Joseph, 127
 função, 113–120
 - bijetora, 116, 117, *veja* permutação, 130, 182
 - contagem, 116
 - chão, *veja* função piso
 - composição, 116–117, 119, 120
 - contra-domínio, *veja* função, imagem
 - definição, 113
 - definição alternativa, 114
 - domínio, 114, 116–118
 - elemento fixo, 119
 - idempotente, 120
 - igualdade, 114
 - imagem, 114, 116, 117
 - de conjunto, 118
 - imagem inversa
 - de conjunto, 118
 - injetora, 115, 117, 118, 164
 - contagem, 115
 - intersecção, 118
 - inversa, 117–119
 - logaritmo, 116, 117
 - notação (\rightarrow), 113
 - permutação, *veja* permutação
 - piso ($\lfloor \cdot \rfloor$), 114
 - projeção, 120
 - quadrado, 113
 - raiz quadrada, 116, 117
 - restrição, 118
 - seno, 114
 - sobrejetora, 115–118
 - contagem, 115
 - solo, *veja* função piso
 - teto ($\lceil \cdot \rceil$), 114
- Gödel, Kurt, 165
 geometria, 15–17
 Goldbach, Christian, 57
 gorila, 49
 grafo, 167–199
 - k -coloração, 198
 - n -cubo, 192
 - árvore, 186, 187, 193
 - definição, 186
 - número de arestas, 187
 - acíclico, 177, 186
 - adjacência
 - matriz, *veja* grafo, matriz de adjacência
 - arco, *veja* grafo, aresta
 - aresta, 167
 - antiparalela, 169–172
 - circular, *veja* grafo, laço
 - como elemento arbitrário, 171, 172
 - como par de vértices, 170
 - como par não ordenado, 170
 - de corte, 185
 - destino, 169, 171
 - direção, 169, 170
 - extremo, 168, 172
 - laço, 169–172
 - múltipla, 169–172, 181
 - orientação, 169, 170
 - origem, 169, 171
 - paralela, 169–172, 181
 - ponte, 186
 - automorfismo, 182
 - bipartido, 187, 191, 192
 - caracterização, 187
 - coloração, 198
 - completo, 187, 193, 196, 198, 199
 - conexo, 195
 - definição, 187
 - caminho, 176, 177, 186
 - comprimento, 187
 - hamiltoniano, 191
 - orientado, 185
 - ciclo, *veja* grafo, circuito

- circuito, 177, 185, 190, 193, 195, 198
 - hamiltoniano, 190
- coloração, 197–199
 - de faces, 197
 - de vértices, 198
- complementar, 180
- complemento, *veja grafo complementar*
- completo, 175, 189, 191, 195, 196
 - coloração, 198
- componente, 184–186
 - fechamento, 184
 - fortemente conexa, 185
- conexidade, *veja grafo conexo*
- conexo, 184–186, 195
 - definição, 184
 - fortemente, 185
 - fracamente, 186
- contagem, 184
- convenções do livro, 172
- de Hamilton, *veja grafo hamiltoniano*
- de Petersen, 195
- definição
 - informal, 167
- desconexo, 185
 - totalmente, 185
- desenho, 167, 169, 188, 193
- diferença, 185
- dual, 197, 198
- em computação, 167
- euleriano, 188–189, 191, 192
 - definição, 188
- face, 193, 197
 - externa, 193
- finito, 169
- fortemente conexo, *veja grafo conexo, fortemente*
- fracamente conexo, *veja grafo conexo, fracamente*
- função
 - de incidência, 169–172
- hamiltoniano, 189–192
 - definição, 190
 - teste, 191
- incidência, 173
 - matriz, *veja grafo, matriz de incidência*
- induzido
 - por vértices, 185
- infinito, 169
- isomorfismo, 181–184, 187, 195
 - algoritmo, 182
 - definição, 182
 - motivação, 181
- laço, 169–173
- matriz
 - de adjacência, 180
 - de entrada, 181
 - de incidência, 181
 - de saída, 181
- número cromático, 198, 199
 - limitantes, 198
- não orientado, 170, 172, 175
- não rotulado, 183
 - contagem, 184
 - enumeração, 183
- orientado, 169–171, 175
- passeio, 175, 176
 - atravessa, 176
 - comprimento, 175, 176
 - concatenação, 176
 - fechado, 177
 - início, 176
 - inverso, 176
 - orientado, 177
 - passa por, 176
 - término, 176
 - trivial, 176, 177
 - vértice interno, 176
 - visita, 176
- percurso, 175–177
- planar, 192–197
 - coloração, 199
 - definição, 193
 - dual, *veja grafo dual*
 - número de arestas, 195
- regular, 174, 175, 177, 187
- relação
 - de adjacência, 173
 - de chegada, 173
 - de dominância, 173
 - de incidência, *veja grafo, incidência*

- de saída, 173
- representação
 - planar, *veja* grafo, desenho
- representação matricial, 180–181
- rotulado, 183
 - contagem, 184
 - enumeração, 183
- sem arestas, 173
- sequência
 - de graus, 175
- simples, 169, 175, 186
- subdivisão, 195
- subgrafo, 178, 184, 195, 196
 - diferença, 180
 - espalhado, 178
 - gerador, 178
 - intersecção, 179
 - união, 179, 184
- tipos, 168–172
- tour
 - de Euler, *veja* grafo, tour euleriano
 - euleriano, 188, 189
- trilha, 176, 177
 - de Euler, *veja* grafo, trilha euleriana
 - euleriana, 188
- vértice, 167
 - adjacente, 173
 - atinge, 173
 - conectado, 184, *veja* grafo, vértice ligado
 - domina, 173
 - grau, 173, 177, 191
 - ligado, 184, 185
 - vizinho, 173
 - vazio, 173, 185
- Guthrie, Francis, 56, 198
- hacker, 214
- Haken, Wolfgang, 56, 198
- Hamilton, William Rowland, 190
- Hasse, Helmut, 102
- Hilbert, David, 162
- hipótese, 30
 - do contínuo, 165
- hotel, 162
- icosaedro, 192
- idempotência
 - da intersecção, 24
 - da união, 24
- igualdade
 - de funções, 114
 - de sequências, 120
- imagem, *veja* relação, contradomínio
 - de conjunto
 - por função, *veja* função, imagem de conjunto
 - inversa, *veja* relação, imagem inversa
- implica, *veja* operador implica
- implicação, *veja* operador implicação
 - lógica, 40–41
- implicação lógica, 40, 47
- inclusão
 - de conjuntos, 19
 - definição, 21
 - estrita
 - definição, 21
 - notação (\subset , \supset), 21
 - notação (\subseteq , \supseteq), 21
- inclusão e exclusão, 156
- indução, 20, 69–84, 156, 157
 - base genérica, 72
 - boa ordenação, 80–82
 - completa, 78–82
 - definição, 69
 - desigualdade, 73, 74
 - equivalência das formas, 81–82
 - forte, *veja* indução completa
 - incorreta, 77–78
 - motivação, 69
 - passo genérico, 74
 - por conjuntos, 71
 - variações, 72–74
- inferência bayesiana, 214–216
 - antecedente, 215
 - consequente, 215
 - fórmula, 214
 - interpretação, 215
 - preconceito, 215
 - probabilidade
 - a posteriori, 215, 216
 - a priori, 215, 216

- infinito
 - como limitante, 26
- inflação, 28
- informação, 216–219
 - capacidade, 216–217
 - versus* quantidade, 218
 - aditividade, 217
 - de sistema físico, 216
 - de sistemas independentes, 217
 - quantidade, 216, 218
 - versus* capacidade, 218
 - definição, 218
 - esperada, *veja* entropia
- injeção, *veja* função injetora
- integral, 136
- inteiro
 - ímpar, 20, 58, 59, 63, 67, 68, 101
 - definição, 56
 - congruência, 108, 109
 - múltiplo, 108
 - par, 57–59, 63, 66, 67, 86, 87, 101, 106
 - definição, 56
 - pitagórico, *veja* tripla pitagórica
 - primo, *veja* primo
- internet, 167, 192
- intersecção, *veja* conjunto
 - de grafos, *veja* grafo, subgrafo, intersecção
- \cap , *veja* conjunto, intersecção
- intervalo
 - de números reais, 26
- inversa
 - de implicação, *veja* proposição inversa
 - de relação, *veja* relação inversa
- iteração
 - de conjunção, 142
 - de disjunção, 142
 - de disjunção exclusiva, 142
 - de intersecção, 142
 - de operação associativa, 142
 - de união, 142
 - vazia, 142
- Java (linguagem), 120
- jogo, 190
- jogos de azar, 202
- Königsberg, 167, 172, 188
- Kempe, Alfred Bray, 198
- Kuratowski, Kasimierz, 195
- lógica, 15, 17–18, 27–53, 55–68
 - clássica, 17
 - de predicados, 43–53
 - proposicional, *veja* cálculo proposicional
 - relação com probabilidade, 205
- lâmpada, 218
- ladrão, 191
- Laplace, Pierre-Simon, 214
- laptop, 29
- lei
 - da adição, 40
 - da associatividade, 38
 - da comutatividade, 38
 - da contrapositiva, 38
 - da distributividade, 38
 - da dominação, 38
 - da idempotência, 38
 - da identidade, 37
 - da implicação, 38
 - da redução ao absurdo, 39, 40
 - da simplificação, 40
 - de De Morgan, 38, 47
 - do modus ponens, 40
 - do modus tollens, 40
 - silogismo disjuntivo, 40
 - silogismo hipotético, 40
- Leibniz, Gottfried Wilhelm, 158
- leis de absorção, 39
- lema, 55
- letra, 168
- limitante
 - de somatória, *veja* somatória, majoração
 - inferior
 - de sequência, 149
 - superior
 - de sequência, 149
- linguagem natural
 - interpretação, 48–49
- lista, *veja* sequência finita
- logaritmo, 133, 136–141
 - como função, *veja* função logaritmo

- Londres, 27
 Lucas, Edouard, 57
- máximo, 105–106
 de dois números, 68
 divisor comum, 17
- média
 aritmética, 62, 67
- métodos de prova, *veja* prova, método
- módulo
 um inteiro, *veja* inteiro, congruência
 uma relação, 109
- múltiplo, 56, 59, 64
 definição, 55
- mínimo, 105–106, 108
 de dois números, 68
- mãe, 49
- macaco, 27, 48, 50
- majoração
 de somatória, *veja* somatória, majoração
- malha viária, 167
- malote, 33
- mamífero, 15, 27
- mapa, 197
- matriz
 booleana, 91
 composição, 92
 conjunção, 92
 disjunção, 92
 intersecção, 92
 produto, 92
 união, 92
 de relação, 91
- maximal, 106–108
- Mersenne, Marin, 57
- minimal, 106–108
- minoração
 de somatória, *veja* somatória, majoração
- modus ponens, 40, *veja* lei do modus ponens
- modus tollens, *veja* lei do modus tollens
- moeda, 204, 206, 216, 217
 falsa, 76, 80
- Moivre, Abraham de, 152
- molécula, 167
- Montevidéu, 28
- morcego, 15, 27
- Morgan, *veja* De Morgan
- mostrador de quilometragem, 217
- multigrafo, 169
- \mathbb{N} (números naturais), *veja* número natural
- número
 ímpar, *veja* inteiro ímpar, 78
 de Fibonacci, 144
 definição, 80
 fórmula, 80
 limite superior, 80
 operações, 80
 somatória, 80
 de fibonacci, 146
 de Mersenne, 57
 divisor, 72
 em binário, 80
 harmônico, 133, 138, 139
 inteiro, 80, 162
 conjunto (\mathbb{Z}), 20
 irracional, 65, 66, 68
 natural, 70, 161
 conjunto (\mathbb{N}), 20
 par, *veja* inteiro par, 161
 pitagórico, *veja* tripla pitagórica
 primo, *veja* primo, 79, 144
 racional, 111
 conjunto (\mathbb{Q}), 20
 real
 conjunto (\mathbb{R}), 20
- número par, 30
- número primo, 17
- números
 cubos, 157
 divisibilidade, 157
 quadrados, 157
- negação, *veja* operador negação, 49, 52
 de quantificador, 47
- negação dupla, 37
- Newton, Isaac, 155
- nota, 74
- notação decimal, 108
- nucleotídeo, 217
- octaedro, 192, 217

- odômetro, 217
- operação
- aritmética, 17
- operador
- associativo, 33, 38
 - bicondicional, *veja* operador equivalência
 - comutativo, 38
 - condicional, *veja* operador implicação
 - conjunção, 59
 - em probabilidade, 204
 - conjunção (“e”, \wedge), 29–30, 33–40, 43
 - de implicação, 94
 - diferença, 67
 - de grafos, *veja* grafo, subgrafo, diferença
 - disjunção, 60
 - em probabilidade, 203, 204
 - disjunção (“ou”, \vee), 29–31, 33–41, 43
 - disjunção exclusiva, 46
 - em probabilidade, 203
 - disjunção exclusiva (\leftrightarrow), 32–33
 - disjunção exclusiva (\oplus), 33–40, 43
 - distributivo, 38
 - dual (\otimes), 43
 - elemento neutro, *veja* elemento neutro
 - equivalência, 56, 62
 - equivalência (\leftrightarrow), 32
 - equivalência (“sse”, \leftrightarrow), 33–41, 43
 - genérico (\odot), 43
 - idempotência, 38
 - implica (“se”, \rightarrow), 30–40, 43
 - implicação
 - prova, *veja* prova de implicação
 - intersecção, 67
 - de grafos, *veja* grafo, subgrafo, intersecção
 - lógico, 28–34
 - não-e (“nand”, $\bar{\wedge}$), 35, 43
 - não-e (“nor”, $\bar{\vee}$), 39
 - não-ou (“nor”, $\bar{\vee}$), 35, 39, 43
 - negação
 - em probabilidade, 203
 - negação (“não”, \neg), 29–31, 33–40, 43
 - precedência, 33–34
 - união, 67
 - de grafos, *veja* grafo, subgrafo, união
- ordenação, 119
- Pólya, George, 77, 184
- palavra, *veja* sequência finita, 168
- papagaio, 50
- par ordenado, 101, 120
 - definição, 25
- Paradoxo
- de Russel, 20
 - do Barbeiro, 20
- paradoxo
- do barbeiro, 34
 - do hotel infinito, 162
 - dos cavalos, 77
- parafuso, 204, 205, 211
- parte
- de partição, 25
- partição, 129
 - de conjunto, *veja* conjunto, partição
 - de um conjunto, 110–111
- Pascal, Blaise, 154, 155
- PBO, *veja* indução, boa ordenação
- Peano, Giuseppe, 70
- pentágono
 - construção, 15
- perfeito, 49
- permutação, 119, 124, 151–152
 - composição, 119
 - contagem, 119, 151
 - das faces de um dado, 119
 - de letras, 151
 - de termos em somatória, 129
 - definição, 119, 151
 - desarranjo, *veja* desarranjo
 - do conjunto vazio, 152
 - dos lados de uma tampa, 119
 - inversa, 119
 - sem elemento fixo, *veja* desarranjo
- \in (pertence), 19
- \notin (não pertence), 19
- pertinência
 - em conjunto, 19
- pessoa conhecida, 180
- Petersen, Julius, 195
- PIC, *veja* indução completa
- PIF, *veja* indução completa
- PIM, *veja* indução, definição

- Pitágoras
 teorema de, 16
- poço de petróleo, 207
- polígono
 convexo, 73
 diagonais, 73
 soma de ângulos, 73
- poliedro
 definição, 192
 platônico, 192
- polinômio
 característico, 146
- ponte
 de Königsberg, 167, 172, 188
- ponto, 16
- poset*, *veja* conjunto parcialmente ordenado
- \ni (possui), 19
- $\not\ni$ (não possui), 19
- postulado, *veja* axioma
- potência
 de binômio, 155
 de conjunto, *veja* conjunto potência
- 2^A , *veja* conjunto potência
- $\mathbb{P}(A)$, *veja* conjunto potência
- preconceito, 215
- predicado, 44, 55
- premissa, 30
- presidente, 86
- primo, 57, 63–66
 definição, 56
- princípio
 da boa ordenação, *veja* indução, boa ordenação
 da complementaridade, 203
 da exaustão, 203
 da exclusão mútua, 203
 da inclusão e exclusão, 156, 204
 da independência, 204, 205
 da indução completa, *veja* indução completa
 da indução forte, *veja* indução completa
 da indução matemática, *veja* indução, definição
 das casas de pombos, *veja* princípio dos escaninhos
 dos escaninhos
 das gavetas, *veja* princípio dos escaninhos
 do pombal, *veja* princípio dos escaninhos
 dos escaninhos, 76
- probabilidade, 201–219
 a posteriori, *veja* inferência bayesiana, probabilidade a posteriori
 a priori, *veja* inferência bayesiana, probabilidade a priori
 como percentagem, 202
 condicional, 213–214
 definição, 213
 inversão, 214
 justificativa, 213
 da conjunção, 204, 205
 da disjunção, 204, 205
 definição, 202
 distribuição, 205, 206
 definição, 205
 degenerada, 219
 entropia, *veja* entropia
 uniforme, 202, 204, 219
 em jogos de azar, 202
 fórmula de Bayes, *veja* inferência bayesiana
 inferência bayesiana, *veja* inferência bayesiana
 justificativa, 201
 princípio da complementaridade, 203
 princípio da exaustão, 203
 princípio da exclusão mútua, 203
 princípio da inclusão e exclusão, 204
 princípio da independência, 204, 205
 princípio de exclusão e inclusão, 205
 relação com lógica, 205
 subjetividade, 202
 teorema de Bayes, *veja* inferência bayesiana
 variável aleatória, *veja* variável aleatória
- problema
 das quatro cores, *veja* grafo, coloração de faces
- produtória, 140–141, 146
 analogia com somatória, 141
 básica, 140
 de constante, 140
 de exponenciais, 141
 de potências, 140
 de progressão aritmética, 140, 141
 definição, 140
 fórmula, 140

- majoração, 141
- manipulação, 141
- vazia, 140
- via logaritmos, 141
- produtório, *veja* produtória
- produto
 - cartesiano, 109, 113
- produto cartesiano, 25, 85
- ênupla, 122
- de n conjuntos, 122
- definição, 25
- iterado, 122
- par ordenado, 25, 122
- progressão
 - aritmética, 145
 - definição, 144
 - incremento, 144
 - passo, 144
 - termo inicial, 144
 - geométrica, 146
 - definição, 144
 - razão, 144
 - termo inicial, 144
- proposição
 - aberta, 43–51
 - atômica, 28
 - auto-referente, 34
 - contraditória, *veja* contradição
 - contrapositiva, 31, 34, 35
 - definição, 27
 - fechada, 44, 51
 - inversa, 31, 35
 - mais forte, 31
 - mais fraca, 31
 - possível, 30
 - recíproca, 31, 35
 - simples, 28
 - tautológica, *veja* tautologia
 - transformação, 36
 - viável, 30
- prova, 17, *veja* demonstração
 - construtiva, 63–65
 - de conjunção, 59
 - de disjunção, 67
 - de equivalência, 61–62, 67
 - de existência e unicidade, 68
 - de falsidade, 66
 - de implicação, 57–60, 67
 - direta, 59
 - hipótese disjuntiva, *veja* prova por casos
 - tese conjuntiva, 59
 - de quantificador existencial, 62–68
 - de quantificador universal, 62–63, 67, 68
 - estratégia, *veja* prova, método
 - existência e unicidade, 65–66
 - implicação
 - contrapositiva, 58
 - direta, 58
 - por absurdo, 59
 - indireta, *veja* prova, implicação por absurdo
 - método, 57–68
 - não construtiva, 65
 - por absurdo, *veja* prova, implicação por absurdo, 65
 - por casos, 60, 68
 - por contra-exemplo, 66–67
 - por contradição, *veja* prova, implicação por absurdo
 - por exemplo, 63
 - por partes, 59
 - por vacuidade, 63, 94
 - qualidades, 57
 - técnica, *veja* prova, método
- Python, 120
- Q (números racionais), *veja* número racional
- quádrupla, *veja* ênupla, 123
- quíntupla, *veja* ênupla
- quadrado
 - monotonicidade, 67
- quadrado perfeito, 63, 67, 68, 86
- quando, *veja* operador implica
- quantificador
 - de existência única, 46
 - em conjunto vazio, 46
 - escopo, 52
 - existencial, 45–47, 50, 63
 - múltiplo, 62
 - universal, 44–47, 50
 - suspensão, 62

- quebra-cabeças, 188, 189, 192
 queijo, 52
- \mathbb{R} (números reais), *veja* número real
 régua e compasso, 15
 rótulo, 119
 raiz quadrada, 85
 como função, *veja* função raiz quadrada
 como relação, 113
 rato, 52
 razão áurea, 146
 recíproca, *veja* proposição recíproca
 recíproco
 de um número, 80
 recho, 96
 recorrência, 144–150
 aditiva
 resolução, 145
 linear
 homogênea, 146
 não homogênea, 148
 termo independente, 148
 majoração, 149–150
 minorção, 149–150
 multiplicativa
 resolução, 146
 resolução, 145–149
 rede, 186
 redução ao absurdo, 39, 40, *veja* prova, implicação
 por absurdo
 refutação, *veja* conjetura refutada
 regra de inferência, 15
 relação, 85–111
 anti-simétrica, 93–96, 100, 103, 105
 aproximadamente igual, 111
 binária, 85
 completa, 109
 composição, 94, 116, 119, 125, 126
 associatividade, 91
 com identidade, 89
 com inversa, 89
 de potências, 91
 definição, 88, 89
 distributiva sobre união, 91
 domínio, 89
 e inclusão, 90
 e intersecção, 91
 em forma matricial, 92
 imagem, 89
 inversa da, 90
 não-comutatividade, 89
 notação alternativa, 89
 potência, 90
 repetida, *veja* potência
 composição (\circ), 88–91
 conjunção de, 92
 contém (\supseteq), 87
 contém estritamente (\supset), 87
 contagem, *veja* contagem de relações
 contido, 101, 103, 107–109
 contido (\subseteq), 86
 contradomínio, *veja* relação, imagem
 de adjacência, 183
 de equivalência, 108–111, 118, 183, 184
 classe, *veja* classe de equivalência
 definição, 108
 entre pares, 111
 de ordem, 100–108, 164
 alfabética, 104, 106
 definição, 100
 entre pares, 101, 104
 estrita, 103, 104
 lexicográfica, 104
 parcial, 105
 subcadeia, 101
 total, 103–105, 119
 união, 101
 definição, 85
 dentro de, 103
 diagrama, 85
 de Hasse, 102
 disjunção de, 92
 divisível, 108
 divisibilidade, 101
 domínio, 86
 entre números, 17
 fecho, *veja* fecho
 fecho simétrico, 173
 função, *veja* função
 identidade, 87, 109

- igual (=), 87
- igualdade, 87
- imagem, 86
 - de conjunto, 118
- imagem inversa, 88
 - de conjunto, 118
- intersecção de, 92
- inversa, 87, 106, 117, 119, 124
- irreflexiva, 93–96, 103
- maior, 101
- maior ou igual, 106
- menor, 86, 101
- menor (<), 86, 87
- menor ou igual, 100, 103, 106
- menor ou igual (\leq), 86
- menor que, 104
- n -ária, 122–126
 - i -ésimo domínio, 122
 - definição, 122
 - grau, 122
 - junção, 124–126
 - ordem, 122
 - permutação de componentes, 124
 - projeção, 123, 124
 - restrição, 124
- paralela, 108
- pertence (\in), 86, 87
- possui (\ni), 87
- potência, 91, 95, 97, 99
- raiz quadrada, 113
- reflexiva, 93–96, 99, 100, 105, 108
- representação matricial, 91–93, 95–96
- restrição, 87, 101, 118
- simétrica, 93–96, 108, 171
- sobre, 86
- tipos, 93–96
- transitiva, 93–95, 100, 102, 103, 105, 108
- união de, 92
- vazia, 86
- repetição, *veja* iteração
- representante
 - de classe de equivalência, 110
- restrição
 - de relação, *veja* relação, restrição
- retórica, 15
- reta, 16
 - dividindo plano, 70, 145
 - paralela, 16, 108
 - perpendicular, 16
- reunião, 30
- Rio de Janeiro, 27
- Robertson, Neil, 56, 198
- ruminante, 50
- Russel, Bertrand, 20
- séptupla, *veja* ênupla
- série, *veja* somatória infinita
- Sócrates, 15
- sêxtupla, *veja* ênupla
- síntese de operadores, 41–43
- Sanders, Daniel, 56
- Sanders, Daniel P., 198
- Schröder, Ernst, 164
- se e somente se, *veja* operador equivalência
- selos, 74
- seno, 114
- sentença declarativa, 27
- sequência, 163
 - índice, 120, 143
 - inicial, 120, 121, 143
 - bi-infinita, 143
 - comprimento, 121
 - de bits, 106
 - elemento, 143
 - índice, 120, 143
 - valor, 120, 143
 - finita, 120–122
 - comprimento, 121
 - concatenação, 121
 - definição, 120
 - notação (\cdot, \cdot, \dots) , 120
 - notação $[\cdot, \cdot, \dots]$, 120
 - notação $\langle \cdot, \cdot, \dots \rangle$, 120
 - vazia, *veja* sequência vazia
- igualdade, 120
- infinita, 143–150
 - índice inicial, 143
 - completando, 143
 - definição, 143
 - dos primos, 144

- por fórmula, 143
 - n -ésimo termo, 120
 - notação x_n , 120
 - ordem dos termos, 120
 - repetição de termos, 120
 - termo, 120, 143
 - índice, 120, 143
 - geral, 143
 - valor, 120, 143
 - vazia, 104, 121
 - comprimento, 121
 - concatenação, 121
 - vs. conjunto, 120
- Seymour, Paul, 56
- Seymour, Paul D., 198
- Shannon, Claude, 216
- sigma (Σ), *veja* somatória
- silogismo
 - disjuntivo, 40
 - hipotético, 40
- sistema binário, 216
- sistema completo, 42–43
- soma, *veja* somatória
- somatória, 127–140
 - índice, 127, 132
 - índice final
 - infinito, 139
 - associatividade, 129, 130
 - básica, 128
 - comutatividade, 129
 - de ímpares, 127
 - de constante, 128
 - de cubos, 73
 - de exponencial, 128, 131, 132
 - de frações, 131
 - de números de Fibonacci, 132
 - de PG, 72
 - de potências, 128, 130, 131, 139
 - de potências crescentes, 131
 - de potências de 2, 128, 131
 - de primos, 127, 129
 - de progressão geométrica, 134
 - de progressão aritmética, 128, 130, 140, 141
 - de progressão geométrica, 128, 131, 132, 139, 140
 - de quadrados, 130, 131
 - de senos, 131
 - decomposição de domínio, 129
 - definição, 127
 - distributividade, 129, 130, 133
 - divergente, 207
 - domínio, 128
 - fórmula, 128
 - fator comum, 129
 - fatoração, 133
 - índice final, 128
 - índice inicial, 128
 - infinita, 139–140
 - dos inversos, 207
 - limitante, *veja* somatória, majoração
 - múltipla, 132–134
 - definição, 132
 - troca de ordem, 132, 133
 - majoração, 134–139
 - pelo maior termo, 134
 - por indução, 134
 - por integral, 136–139
 - por somatória infinita, 139
 - termo a termo, 134, 139
 - manipulação, 128–132
 - minoração, *veja* somatória, majoração
 - notação, 127
 - ordem dos termos, 129
 - produto, 133
 - propriedades, 129
 - telescópica, 130, 131
 - termo, 127
 - troca de índice, 128–130, 132
 - troca de domínio, 130, 132
 - vazia, 128
- somatório, *veja* somatória
- Stirling, James, 152
- sub-conjunto, *veja* inclusão
 - definição, 21
 - próprio
 - definição, 21
- subcadeia, 122
- subconjunto, 67
- subsequência, 122, 143

- Távola Redonda, 189
 tabela-verdade, 29, 30, 32, 35–37, 39–43
 tampa de caixa, 119
 tanque, 33
 tatu, 145, 147
 tautologia, 36, 37, 40, 47
 taxa de juros, 27, 28
 Tchebychev, Pafnuti, 211
 teorema, 16, 55
 da infinidade de primos, 65
 de Bayes, *veja* inferência bayesiana
 de Cantor, 163–164
 de Euler
 para grafos planares, 194
 para tours em grafos, 188
 de Fermat, *veja* conjectura de Fermat
 de Kuratowski, 195
 de Pólya, 184
 do deserto de primos, 64
 teoria
 da computabilidade, 17
 da informação, 17, *veja* informação
 da probabilidade, 17
 de conjuntos, 17
 dos conjuntos, 19–26
 dos grafos, *veja* grafo
 tese, 30
 tetraedro, 192
 Thomas, Robin, 56, 198
 tijolos, 29
 triângulo equiângulo, 49
 treliça, 167
 triângulo, 16
 congruência, 16
 retângulo, 16
 tripla, 122, *veja* ênupla, 123
 troca, *veja* permutação
 troco, 74
 união, *veja* conjunto
 de grafos, *veja* grafo, subgrafo, união
 \cup , *veja* conjunto, união
 \mathcal{U} , *veja* conjunto universal
 urna, 72
 vacuidade, 46
 valor absoluto, 68
 valor lógico, 27
 falso, 142
 verdadeiro, 142
 valor-verdade, 27
 variável, 17
 aleatória, 205–212
 contínua, 206
 discreta, 206
 amarrada, 51, 55
 lógica, 28
 livre, 51, 55
 variável aleatória
 coeficiente de correlação, *veja* correlação
 correlação, 212
 covariância, 212
 definida por fórmula, 206, 208
 desvio padrão, 211–212
 definição, 211
 teorema de Tchebychev, 211
 esperança, *veja* variável aleatória, valor esperado
 média, *veja* variável aleatória, valor esperado
 mediana, 208–209
 moda, 209–210
 teorema de Tchebychev, 211
 valor esperado, 206–208
 com distribuição uniforme, 207
 função afim, 208
 função linear, *veja* função afim
 função não linear, 208
 infinito, 207
 soma, 208
 valor médio, *veja* variável aleatória, valor esperado
 valor mais provável, *veja* moda
 variância, 210–212
 definição, 210
 função afim, 211
 infinita, 210
 justificativa, 210
 sinal, 210
 soma, 211
 vetorial

valor esperado, 208
variavel aleatória
 vetorial, 208
Venn, John, 23
voto, 34

xadrez, 192

 \mathbb{Z} (números inteiros), *veja* número inteiro
zebra, 50
Zermelo, Ernest, 19
zoológico, 27