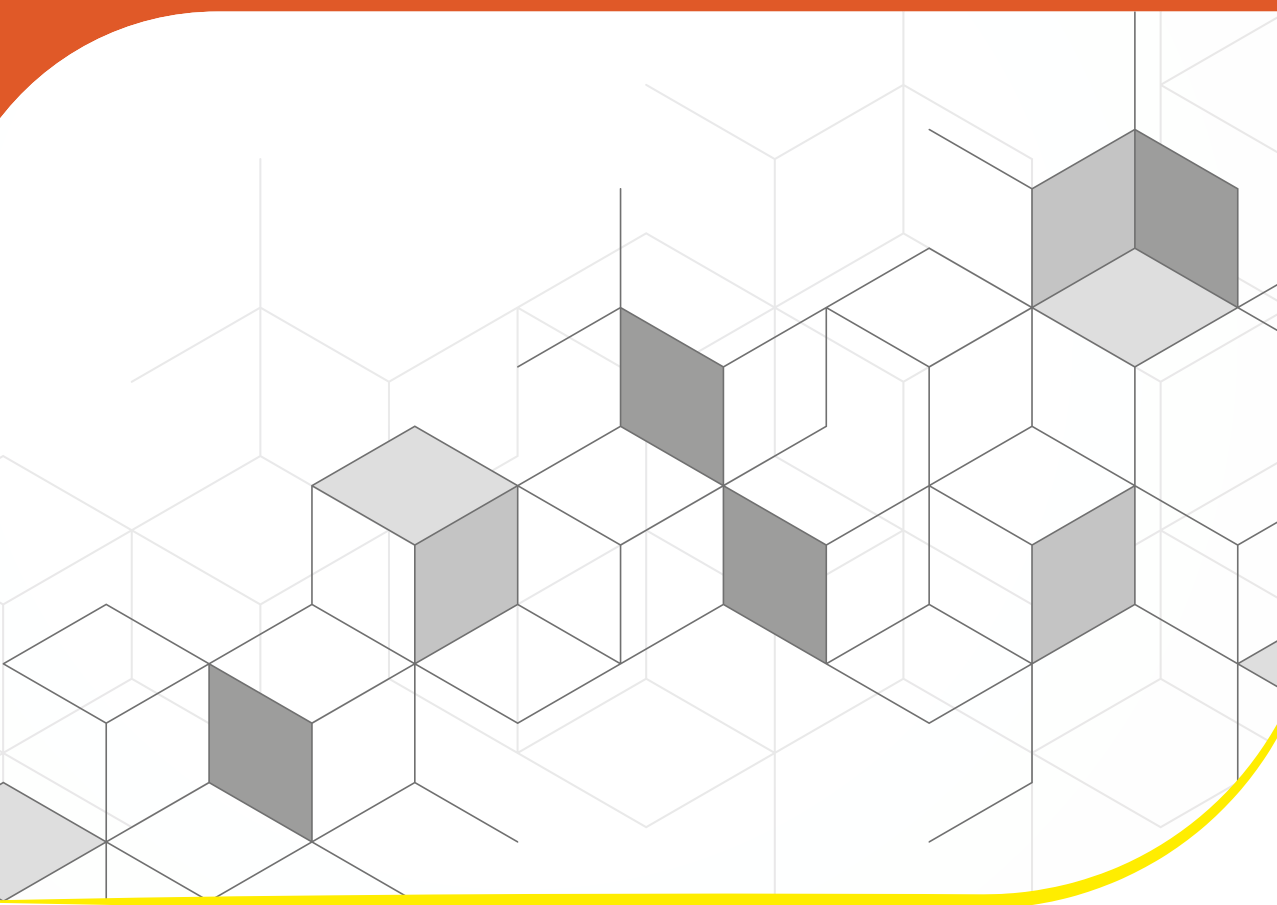
MARCUS VINICIUS MIDENA RAMOS
JOÃO JOSÉ NETO
ITALO SANTIAGO VEGA

LINGUAGENS FORMAIS

Teoria e conceitos



Blucher

LINGUAGENS FORMAIS
Teoria e conceitos

Marcus Vinicius Midena Ramos
João José Neto
Italo Santiago Vega

Linguagens formais: teoria e conceitos

Publisher Edgard Blücher
Editores Eduardo Blücher e Jonatas Eliakim
Coordenação editorial Andressa Lira
Produção editorial Ariana Corrêa
Diagramação Marcus Vinicius Midena Ramos
Revisão de texto Maurício Katayama
Capa Laércio Flenic
Imagem da capa iStockphoto

Editora Blucher
Rua Pedroso Alvarenga, 1245, 4º andar
CEP 04531-934 – São Paulo – SP – Brasil
Tel.: 55 11 3078-5366
contato@blucher.com.br
www.blucher.com.br

Dados Internacionais de Catalogação na Publicação (CIP)
Angélica Ilacqua CRB-8/7057

Ramos, Marcus Vinicius Midena
Linguagens formais : teoria e conceitos / Marcus Vinicius Midena Ramos, João José Neto, Italo Santiago Vega. - São Paulo : Blucher, 2023.
608 p.: il.

Bibliografia
ISBN 978-65-5506-716-3

1. Engenharia da computação 2. Matemática - Processamento de dados 3. Teoria dos autômatos 4. Linguagens formais I. Título II. José Neto, João III. Vega, Italo Santiago

CDD 004
23-3483

Índice para catálogo sistemático: 1. Engenharia da computação

Conteúdo

Capítulo 1

Elementos de matemática discreta

As **linguagens formais** (ou linguagens estruturadas em frases) podem ser vistas como conjuntos. Consequentemente, muito da teoria e dos principais resultados da área de linguagens formais está baseado na ainda mais fundamental teoria dos conjuntos da matemática discreta. A teoria dos conjuntos é relativamente extensa, e dela serão apresentados neste capítulo apenas os tópicos, conceitos e definições que se mostram mais importantes para a fundamentação e o estudo dos capítulos seguintes.

Além disso, relações e funções são de especial importância para descrever as relações entre os objetos de estudo, e por isso são assuntos contemplados neste capítulo.

Da mesma forma, é preciso conhecer um pouco de lógica e de prova de teoremas para poder compreender o significado dos enunciados e as estratégias de provas usadas no texto.

Completam a relação de tópicos da matemática discreta que são relevantes para linguagens formais e autômatos conceitos básicos de grafos e árvores.

1.1 Conjuntos

Um **conjunto** é uma coleção de elementos em que não são consideradas ocorrências múltiplas deles nem há relação de ordem entre eles.

Exemplo 1.1 A inclusão do elemento $\diamondsuit$ no conjunto $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ resulta no próprio conjunto $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, pois ele já faz parte do conjunto e, portanto, não deve ser considerado novamente. Por outro lado, o conjunto $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ é igual ao conjunto $\{\diamondsuit, \clubsuit, \spadesuit, \heartsuit\}$, uma vez que não existe relação de ordem entre os elementos que os compõem. ⋆

Alguns conjuntos podem ser especificados através da simples **enumeração** de todos os seus elementos, denotados entre chaves e separados por vírgulas.

Exemplo 1.2 O conjunto formado pelos elementos $0, 1, 2, 3$ é representado por $\{0, 1, 2, 3\}$. O conjunto $\{a, b, c, d, e, f\}$ é formado pelas seis primeiras letras do alfabeto romano. O conjunto $\{01, 231, 33, 21323\}$ contém os elementos $01, 231, 33$ e 21323. ⋆

Conjuntos podem ser referenciados através de nomes, arbitrariamente escolhidos.

Exemplo 1.3 $X = \{0, 1, 2, 3\}$, $Y = \{a, b, c, d, e, f\}$. Assim, os nomes X e Y passam a denotar os conjuntos correspondentes. ⋆

O número de elementos contido em um conjunto A é denotado por $|A|$.

Exemplo 1.4 No Exemplo 1.3, $|X| = 4$, $|Y| = 6$. ⋆

Os símbolos $\in$ e $\notin$ servem para denotar se um determinado elemento **pertence** ou **não pertence** a um conjunto, respectivamente.

Exemplo 1.5 No Exemplo 1.3, $0 \in X$, $5 \notin X$, $2 \notin Y$, $b \notin X$, $c \in Y$, $h \notin Y$. ⋆

Conjuntos podem conter um número finito ou infinito de elementos. No primeiro caso, o conjunto pode ser denotado enumerando-se (relacionando-se explicitamente) todos os elementos que o compõem, como foi feito para os conjuntos X e Y do Exemplo 1.3, que são **conjuntos finitos**.

Conjuntos infinitos podem ser denotados através da especificação (formal ou informal) de regras ou propriedades que devem ser satisfeitas por todos os seus elementos, possibilitando assim a sua identificação precisa e completa a partir de uma especificação finita.

Exemplo 1.6 $P = \{x \mid x \text{ é um número primo}\}$, $Q = \{y \mid \exists n \text{ inteiro tal que } y = n^2\}$. O primeiro exemplo deve ser lido da seguinte forma: "P é o conjunto formado pelos elementos x, tal que x é um número primo". Em outras palavras, P é o conjunto, infinito, formado por todos os números primos: $\{2,3,5,7,11,13,17...\}$. O conjunto Q, também infinito, é formado por todos os números que correspondem ao quadrado de algum número inteiro: $\{0,1,4,9,16...\}$. ⋆

Quando um conjunto é especificado a partir de regras, o símbolo "|" deve ser lido como "tal que", e serve para introduzir as condições que devem ser satisfeitas pelos membros do conjunto, que assim tornam-se conhecidos.

O conjunto que não contém nenhum elemento recebe o nome de **conjunto vazio**. O conjunto vazio é denotado por $\emptyset$ ou ainda por $\{\}$. Assim, $\{\} = \emptyset$. Por definição, $|\emptyset| = 0$.

Dois conjuntos são ditos **idênticos**, ou simplesmente **iguais**, se eles contêm exatamente os mesmos elementos. A igualdade de dois conjuntos é denotada através do símbolo "=".

Exemplo 1.7 Considere $Z = \{a,b\}$ e $W = \{b,a\}$. Então, $Z = W$. ⋆

A teoria de conjuntos apresentada nesta seção é um resumo da chamada Teoria Ingênua de Conjuntos (do inglês *Naïve Set Theory*) elaborada por Georg Cantor no final do século XIX. Tal teoria, apesar de simples, permite enunciar alguns paradoxos, entre os quais o mais famoso é o Paradoxo de Russell, proposto por Bertrand Russell em 1901, e que envolve apenas os conceitos de formação de conjunto e de pertencimento:

> Seja S o conjunto formado por todos os conjuntos que não são elementos de si mesmos, e considere a pergunta: "S é elemento de si mesmo?"

Para tentar responder a essa pergunta, pode-se considerar duas situações distintas. Na primeira, supõe-se que S seja um elemento de si mesmo. Então, de acordo com a definição, S não deveria fazer parte de S, uma vez que S contém apenas conjuntos que não são elementos de si mesmos. Por outro lado, pode-se supor o caso contrário, ou seja, que S não seja um elemento de si mesmo. Então, pela definição, S se qualifica como um elemento de si mesmo. Portanto, qualquer que seja o caso que se considere, temos uma contradição. Logo, a hipótese é falsa e não existe um conjunto S com tal característica.

A fim de evitar a formulação de paradoxos como esse, foram desenvolvidas teorias de conjuntos alternativas, como é o caso da Teoria de Tipos do próprio Russell e também a Teoria Axiomática de Zermelo, que posteriormente serviu de base para a Teoria Axiomática de Zermelo-Fraenkel com o Axioma da Escolha (ZFC). Essa última é considerada um dos principais fundamentos da matemática moderna.

Um conjunto A é dito "**contido** em um conjunto B", condição esta denotada através do símbolo "$\subseteq$", se todo elemento de A for também elemento de B. Neste caso diz-se, equivalentemente, que "A é um **subconjunto** de B" ou, ainda, que "B **contém** A". Os conjuntos $\emptyset$ e A são, por definição, subconjuntos de qualquer conjunto A. Note que $\emptyset \subseteq \emptyset$.

Exemplo 1.8 Para os conjuntos $A = \{b,c,d\}$, $B = \{a,b,c,d,e\}$ e $C = \{e,a,d,b,c\}$ tem-se que $A \subseteq B$ e $B \subseteq C$. Portanto, pode-se dizer que A está contido em B e em C, que A é subconjunto de B e de C, que C contém A e B e, ainda, que B e C são subconjuntos um do outro ou que estão contidos um no outro. B e C, por outro lado, não estão contidos em A. ⋆

Dois conjuntos M e N são iguais se e somente se $M \subseteq N$ e $N \subseteq M$, e tal igualdade é denotada por $M = N$. A **desigualdade** de dois conjuntos é expressa através do símbolo "$\neq$", ocorrendo, portanto, quando no máximo apenas uma das duas condições $M \subseteq N$ e $N \subseteq M$ for verdadeira.

Exemplo 1.9 No Exemplo 1.8, $A \subseteq B$, porém $A \neq B$. Como $B \subseteq C$ e $C \subseteq B$, então $B = C$. ⋆

Se $M \subseteq N$ e $M \neq N$, diz-se que M é um **subconjunto próprio** de N. O símbolo $\subset$ denota essa condição: $M \subset N$. O conjunto $\emptyset$ é subconjunto próprio de qualquer conjunto, exceto do próprio conjunto $\emptyset$.

Exemplo 1.10 No Exemplo 1.8, A é subconjunto próprio de B, porém B não é subconjunto próprio de C. Logo, $A \subset B$. ⋆

Algumas operações importantes sobre conjuntos são apresentadas a seguir.

Conjunto potência ou "powerset"

Denotado por 2^A, onde A é um conjunto. Essa operação é utilizada para designar o conjunto formado por todos os possíveis subconjuntos de A:

$$2^A = \{B \mid B \subseteq A\}$$

Para conjuntos A finitos, $|2^A| = 2^{|A|}$. Note que $2^{\emptyset} = \{\emptyset\}$.

Exemplo 1.11 Para $A = \{0,1,2\}$, temos $2^A = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$. Além disso, $|A| = 3$ e $|2^A| = 2^3 = 8$. ⋆

União

A união de dois conjuntos A e B corresponde ao conjunto formado por todos os elementos contidos em cada um dos dois conjuntos A e B. Elementos repetidos em ambos os conjuntos são considerados uma única vez no conjunto união:

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

Trata-se de uma operação associativa, ou seja, uma operação para a qual vale a propriedade:

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

A generalização da operação de união é denotada da seguinte forma:

$$\bigcup_{i=0}^{n} A_i = A_0 \cup A_1 \cup A_2 \cup \ldots \cup A_n$$

A operação de união é também comutativa, ou seja:

$$A \cup B = B \cup A$$

para quaisquer conjuntos A e B.

O conjunto vazio $\emptyset$ é o **elemento neutro** da operação de união. Para todo conjunto A, $A \cup \emptyset = A$.

Exemplo 1.12 $\{a,b\} \cup \{c,d\} = \{a,b,c,d\}$. $\{a,b,c\} \cup \{c,d\} = \{a,b,c,d\}$. $\{a,b,c,d\} \cup \emptyset = \{a,b,c,d\}$. ⋆

Intersecção

Define-se a intersecção de dois conjuntos A e B como sendo a coleção de todos os elementos comuns aos dois conjuntos:

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

Também em decorrência da associatividade dessa operação, a sua generalização é denotada de forma similar ao caso da união:

$$\bigcap_{i=0}^{n} A_i = A_0 \cap A_1 \cap A_2 \cap \ldots \cap A_n$$

Da mesma forma que a união, a operação de intersecção é também comutativa:

$$A \cap B = B \cap A$$

para quaisquer conjuntos A e B.

A intersecção de qualquer conjunto com o conjunto vazio produz como resultado o próprio conjunto vazio, ou seja, $A \cap \emptyset = \emptyset$. O conjunto vazio, nesse caso, é denominado **aniquilador** da operação de intersecção.

Exemplo 1.13 $\{a,b,c\} \cap \{c,d\} = \{c\}$. $\{a,b,c,d\} \cap \{c,d\} = \{c,d\}$. $\{a,b\} \cap \{c,d\} = \emptyset$. $\{a,b,c,d\} \cap \emptyset = \emptyset$. ⋆

Dois conjuntos A e B são ditos **disjuntos** se $A \cap B = \emptyset$.

Exemplo 1.14 Os conjuntos $\{a,b,c\}$ e $\{c,d\}$ não são disjuntos, pois $\{a,b,c\} \cap \{c,d\} = \{c\} \neq \{\}$. Os conjuntos $\{a,b\}$ e $\{c,d\}$ são disjuntos, pois $\{a,b\} \cap \{c,d\} = \emptyset$. ⋆

Diferença

Define-se a diferença entre dois conjuntos A e B (nesta ordem) como sendo o conjunto formado por todos os elementos de A não pertencentes ao conjunto B. Denota-se esse conjunto como:

$$A - B = \{x \mid x \in A \text{ e } x \notin B\}$$

Exemplo 1.15 $\{a,b,c\} - \{c,d\} = \{a,b\}$. $\{a,b\} - \{a,b,c\} = \emptyset$. $\{a,b,c\} - \{d,e\} = \{a,b,c\}$. $\{c,d\} - \{a,b,c\} = \{d\}$. $\{a,b,c\} - \{a,b\} = \{c\}$. $\{d,e\} - \{a,b,c\} = \{d,e\}$. ⋆

Essa operação não é associativa (no caso geral, $A - (B - C) \neq (A - B) - C$) nem comutativa (no caso geral, $A - B \neq B - A$).

Exemplo 1.16 Sejam $X = \{a,b,c\}, Y = \{a,b\}$ e $Z = \{a\}$. Então, $X - (Y - Z) \neq (X - Y) - Z$. De fato, $X - (Y - Z) = \{a,c\}$ e $(X - Y) - Z = \{c\}$. Por outro lado, $X - Y \neq Y - X$. De fato, $X - Y = \{c\}$ e $Y - X = \emptyset$. ⋆

Note, no entanto, que se $A = B = C$, então a operação se torna comutativa (produzindo sempre $\emptyset$ como resultado), mas continua sendo não associativa.

Complementação

Define-se a complementação de um conjunto A em relação ao conjunto B, $A \subseteq B$, como sendo o conjunto de todos os elementos de B que não pertencem a A. Denota-se esse conjunto como:

$$\overline{A}_B = B - A$$

Muitas vezes essa operação é definida para um conjunto A em relação a um outro conjunto B subentendido e, nesse caso, escreve-se simplesmente:

$$\overline{A} = B - A$$

Diz-se, nesse caso, que o conjunto subentendido é o conjunto universo da operação. O resultado da operação é conhecido simplesmente como **complemento** de A.

Exemplo 1.17 Sejam $A = \{a,b,c\}$, $B = \{a,b,c,d\}$ e $C = \{d,c,a,b\}$. Então, $\overline{A}_B = \{d\}$ e $\overline{B}_C = \emptyset$. Sendo $D = \{a,b,c,d,e\}$ o conjunto universo, $\overline{A} = \{d,e\}$, $\overline{B} = \overline{C} = \{e\}$ e $\overline{D} = \emptyset$. ⋆

Produto cartesiano

O produto cartesiano de dois conjuntos é o conjunto formado por todos os pares ordenados (a,b), em que a é um elemento de A, e b um elemento de B:

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

Um **par ordenado** é uma representação de dois elementos separados por vírgula e delimitados por parênteses, como em (a,b). Tal representação implica uma relação de ordem em que o elemento a é anterior ao elemento b. Consequentemente, se $a \neq b$, então $(a,b) \neq (b,a)$.

Se A e B são conjuntos finitos, então $|A \times B| = |A| * |B|$. Para todo conjunto A, $A \times \emptyset = \emptyset$.

A generalização dessa operação é denotada:

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \mid a_i \in A_i \text{ para } 1 \leqslant i \leqslant n\}$$

Exemplo 1.18 Sejam $A = \{a,b,c\}$ e $B = \{0,1\}$. Então $A \times B = \{(a,0),(a,1),(b,0),(b,1),(c,0),(c,1)\}$ e $|A \times B| = |A| * |B| = 3 * 2 = 6$. ⋆

Essa operação não é associativa (no caso geral, $A \times (B \times C) \neq (A \times B) \times C$) nem comutativa (no caso geral, $A \times B \neq B \times A$).

Exemplo 1.19 Considere novamente o Exemplo 1.18 e suponha $C = \{\diamondsuit\}$. Estruturalmente, é fácil perceber que $A \times (B \times C) \neq (A \times B) \times C$. De fato, $(a,(0,\diamondsuit)) \in A \times (B \times C)$ e $(a,(0,\diamondsuit)) \notin (A \times B) \times C$. Por outro lado, $((a,0),\diamondsuit) \in (A \times B) \times C$ e $((a,0),\diamondsuit) \notin A \times (B \times C)$. No que se refere à comutatividade, basta perceber que $B \times A = \{(0,a),(0,b),(0,c),(1,a),(1,b),(1,c)\}$ e, portanto, $A \times B \neq B \times A$. ⋆

Finalmente, observe que, se $A = B = C$, então a operação se torna comutativa mas continua não associativa. De fato, $A \times (A \times A) \neq (A \times A) \times A \neq A \times A \times A$.

Partição

Define-se **partição** de um conjunto A como sendo qualquer coleção formada por n subconjuntos não vazios de A, $n \geqslant 1$, tal que:

$$A = \bigcup_{i=0}^{n} A_i \quad \text{e} \quad \bigcup_{i=0}^{n} \left(\bigcup_{j=0}^{n, j \neq i} A_i \cap A_j \right) = \emptyset$$

ou seja, a união das partes (os conjuntos A_i) deve formar o todo (o conjunto A) e, além disso, a intersecção entre quaisquer duas partes consideradas (A_i e A_j) é sempre vazia.

Exemplo 1.20 Seja $A = \{a,b,c,d\}$. Então, $\{\{a,b\},\{c,d\}\}$ é uma partição de A. Da mesma forma, o conjunto $\{\{a\},\{b\},\{c\},\{d\}\}$, bem como $\{\{a,b,c,d\}\}$, entre vários outros. ⋆

A seguir serão apresentados quatro importantes resultados acerca de conjuntos, os dois primeiros conhecidos como **Leis de De Morgan**, os quais serão úteis na demonstração de outros teoremas mais adiante no texto.

Teorema 1.1 (Leis de De Morgan) "Sejam A e B dois conjuntos quaisquer. Então $A \cap B = \overline{\overline{A} \cup \overline{B}}$ e $A \cup B = \overline{\overline{A} \cap \overline{B}}$."

A prova algébrica da primeira lei ($A \cap B = \overline{\overline{A} \cup \overline{B}}$, ou representação da intersecção por meio da complementação e da união) procede da seguinte forma:

- Deve-se provar que $x \in A \cap B \Rightarrow x \in \overline{\overline{A} \cup \overline{B}}$; e também
- Deve-se provar que $x \in \overline{\overline{A} \cup \overline{B}} \Rightarrow x \in A \cap B$.

Para o primeiro caso, temos que se $x \in A \cap B$, então $x \in A$ e $x \in B$. Logo, $x \notin \overline{A}$ e $x \notin \overline{B}$. Portanto, $x \notin \overline{A} \cup \overline{B}$. Consequentemente, $x \in \overline{\overline{A} \cup \overline{B}}$. Para o segundo caso, temos que se $x \in \overline{\overline{A} \cup \overline{B}}$, então $x \notin \overline{A} \cup \overline{B}$. Portanto, (i) $x \notin \overline{A}$ e (ii) $x \notin \overline{B}$. Então, $x \in A$ e $x \in B$. Logo, $x \in A \cap B$.

Para facilitar o entendimento desta prova, basta analisar o Diagrama de Venn da Figura 1.1. Da esquerda para a direita, as áreas hachuradas dos diagramas representam, respectivamente, $\overline{A}, \overline{B}, \overline{A} \cup \overline{B}$ e $\overline{\overline{A} \cup \overline{B}}$.

A prova algébrica da segunda lei ($A \cup B = \overline{\overline{A} \cap \overline{B}}$, ou representação da união por meio da complementação e da intersecção) procede da seguinte forma:

- Deve-se provar que $x \in A \cup B \Rightarrow x \in \overline{\overline{A} \cap \overline{B}}$; e também
- Deve-se provar que $x \in \overline{\overline{A} \cap \overline{B}} \Rightarrow x \in A \cup B$.

Para o primeiro caso, temos que se $x \in A \cup B$, então (i) $x \in A$ e $x \in B$, ou (ii) $x \in A$ e $x \notin B$, ou (iii) $x \notin A$ e $x \in B$. Em outras palavras, (i) $x \notin \overline{A}$ e $x \notin \overline{B}$, ou (ii) $x \notin \overline{A}$ e $x \in \overline{B}$, ou (iii) $x \in \overline{A}$ e $x \notin \overline{B}$. Em qualquer caso, $x \notin \overline{A} \cap \overline{B}$. Logo, $x \in \overline{\overline{A} \cap \overline{B}}$. Para o segundo caso, temos que se $x \in \overline{\overline{A} \cap \overline{B}}$, então $x \notin \overline{A} \cap \overline{B}$. Portanto, (i) $x \notin \overline{A}$, ou (ii) $x \notin \overline{B}$, ou (iii) os dois casos anteriores acontecem simultaneamente. Se (i) for verdade, então conclui-se que $x \in A$. Se (ii) for verdade, conclui-se que $x \in B$. Se (iii) for verdade, conclui-se que os dois casos anteriores são verdadeiros. Em qualquer situação, temos que $x \in A \cup B$.

Para facilitar o entendimento desta prova, basta analisar o Diagrama de Venn da Figura 1.2. Da esquerda para a direita, as áreas hachuradas dos diagramas representam, respectivamente, $\overline{A}, \overline{B}, \overline{A} \cap \overline{B}$ e $\overline{\overline{A} \cap \overline{B}}$. □

Exemplo 1.21 Suponha $X = \{a,b\}, Y = \{b,c\}$ e considere $Z = \{a,b,c\}$. Então, $X \cup Y = \overline{(\overline{X}_Z \cap \overline{Y}_Z)}_Z = \overline{(\{c\} \cap \{a\})}_Z = \overline{\emptyset}_Z = \{a,b,c\}$. Por outro lado, $X \cap Y = \overline{(\overline{X}_Z \cup \overline{Y}_Z)}_Z = \overline{(\{c\} \cup \{a\})}_Z = \overline{\{a,c\}}_Z = \{b\}$. ⋆

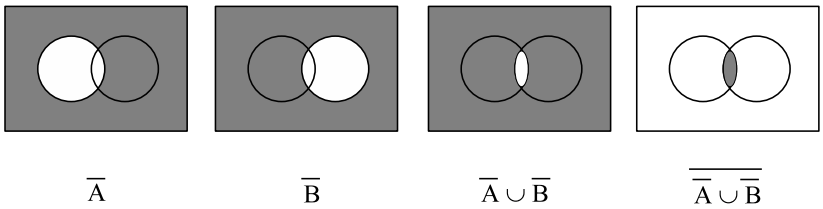


Figura 1.1 Demonstração da Lei de De Morgan para intersecção de conjuntos.

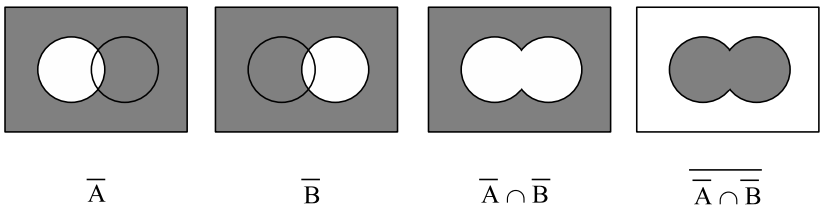


Figura 1.2 Demonstração da Lei de De Morgan para união de conjuntos.

Teorema 1.2 (Igualdade de conjuntos) "Sejam A e B dois conjuntos quaisquer. Então $A = B \Leftrightarrow (A \cap \overline{B}) \cup (\overline{A} \cap B) = \emptyset$."

($\Rightarrow$) Se $A = B$, então $(A \cap \overline{B}) \cup (\overline{A} \cap B) = (A \cap \overline{A}) \cup (\overline{A} \cap A) = \emptyset \cup \emptyset = \emptyset$.
($\Leftarrow$) Se $(A \cap \overline{B}) \cup (\overline{A} \cap B) = \emptyset$, então as duas condições seguintes devem ser simultaneamente satisfeitas:

1. $(A \cap \overline{B}) = \emptyset$;
2. $(\overline{A} \cap B) = \emptyset$.

Considere-se a condição (1) e, além disso, $A \subseteq C$ e $B \subseteq C$, de forma que $\overline{A} = \overline{A}_C$ e $\overline{B} = \overline{B}_C$. Então, existem apenas três possibilidades para representar a relação entre A e B:

i $A \neq B$ e $A \cap B \neq \emptyset$. Logo, $A \cap \overline{B} \neq \emptyset$;
ii $A \neq B$ e $A \cap B = \emptyset$. Logo, $A \cap \overline{B} \neq \emptyset$;
iii $A = B$. Logo, $A \cap \overline{B} = \emptyset$.

No caso da relação (ii), é possível ainda supor que $A = \emptyset$ e $B \neq \emptyset$. Se isso acontecer, então temos que $A \cap \overline{B} = \emptyset$, configurando assim uma possibilidade alternativa para satisfazer a condição (1). No entanto, se isso for verdadeiro, então a condição (2) não poderá ser satisfeita, pois $\overline{A} \cap B \neq \emptyset$. O mesmo raciocínio pode ser aplicado para a condição (2), se $A \neq \emptyset$ e $B = \emptyset$.

Portanto, a única relação possível entre A e B que satisfaz à condição (1) é a relação (iii). Da mesma forma, pode-se facilmente mostrar que (iii) também é a única relação que satisfaz à condição (2), e isso completa a demonstração do teorema. □

Teorema 1.3 (Subconjuntos) "Sejam A e B dois conjuntos quaisquer. Então $A \subseteq B \Leftrightarrow \overline{B} \cap A = \emptyset$."

($\Rightarrow$) Se $A \subseteq B$, então $\forall x \in A, x \in B$. Logo, $\forall x \in A, x \notin \overline{B}$. Portanto, $\overline{B} \cap A = \emptyset$.
($\Leftarrow$) Se $\overline{B} \cap A = \emptyset$, então A e $\overline{B}$ são disjuntos. Logo, $\forall x, (x \in A \wedge x \notin \overline{B}) \vee (x \notin A \wedge x \in \overline{B}) \vee (x \notin A \wedge x \notin \overline{B})$. Ou seja, $\forall x, (x \in A \wedge x \in B) \vee (x \notin A \wedge x \notin B) \vee (x \notin A \wedge x \in B)$. Claramente, portanto, $A \subseteq B$ (veja Figura 1.3).

De outra forma, dados dois conjuntos A e B quaisquer, então todas as possibilidades de relacionamento entre esses conjuntos estão relacionadas a seguir:

1. $A \cap B = \emptyset$, ou
2. $A \cap B \neq \emptyset$, logo:

    a) $A = B$, ou
    b) $A \neq B$, logo:

        i. $A \subset B$, ou
        ii. $B \subset A$, ou
        iii. $A \not\subset B \wedge B \not\subset A \wedge A \cap B \neq \emptyset$

Não é difícil perceber que a condição $\overline{B} \cap A = \emptyset$ é verificada apenas nos casos $A = B$ e $A \subset B$. Em todos os demais, $\overline{B} \cap A \neq \emptyset$. Logo, $A \subseteq B$.

O presente teorema permite representar a relação "subconjunto" por meio das operações de complementação e intersecção. A Figura 1.3 ilustra os passos dessa demonstração.

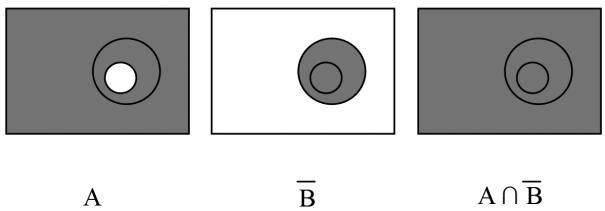


Figura 1.3 Demonstração de $A \subseteq B \Leftrightarrow \overline{B} \cap A = \emptyset$.

□

A menos de ressalva em contrário, ao longo deste texto os nomes de conjuntos serão representados por intermédio das letras maiúsculas do alfabeto romano (A, B, X, Y etc.). Elementos de um conjunto são usualmente denotados através das letras minúsculas do mesmo alfabeto (a, b, c etc.).

Os seguintes conjuntos serão utilizados no restante deste livro:

- $\mathbb{N}$, representando os números naturais $\{0, 1, 2, 3, ...\}$;
- $\mathbb{Z}$, representando os números inteiros $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$;
- $\mathbb{Z}_+$, representando os números inteiros positivos $\{1, 2, 3, ...\}$;
- $\mathbb{Z}_-$, representando os números inteiros negativos $\{..., -3, -2, -1\}$;
- $\mathbb{R}$, representando os números reais;
- $\mathbb{Q}$, representando os números racionais.

Diz-se que um conjunto é **fechado em relação a uma operação** se da aplicação dessa operação a quaisquer membros desse conjunto resultarem sempre elementos que também são membros do mesmo conjunto.

Exemplo 1.22 Considere-se o conjunto $X = \{x \in \mathbb{R} \mid x \geqslant 0\}$ e a operação unária $\sqrt{}$ (raiz quadrada). Qualquer que seja o elemento $x \in X$ considerado, $\sqrt{x}$ é sempre um elemento de X. Portanto, o conjunto X é fechado em relação à operação $\sqrt{}$.

Por outro lado, não se pode dizer o mesmo do conjunto $\mathbb{R}$, uma vez que a operação raiz quadrada não é definida para números negativos. Logo, o conjunto $\mathbb{R}$ não é fechado em relação à operação $\sqrt{}$. ⋆

Exemplo 1.23 Considerem-se os conjuntos dos números inteiros $\mathbb{Z}$, dos números naturais $\mathbb{N}$ e as operações binárias de soma e subtração. Então, as seguintes afirmativas são verdadeiras:

- O conjunto $\mathbb{Z}$ é fechado em relação à operação de soma. De fato, da soma de quaisquer dois elementos de $\mathbb{Z}$ resulta sempre um elemento que também pertence ao conjunto $\mathbb{Z}$.
- O conjunto $\mathbb{Z}$ é fechado em relação à operação de subtração, pois da subtração de quaisquer dois elementos de $\mathbb{Z}$ resulta sempre um elemento que também pertence ao conjunto $\mathbb{Z}$.
- O conjunto $\mathbb{N}$ não é fechado em relação à operação de subtração: nem toda subtração de dois elementos arbitrários de $\mathbb{N}$ fornece como resultado um elemento que também pertença ao conjunto $\mathbb{N}$. Assim, por exemplo, se $1 \in \mathbb{N}$ e $2 \in \mathbb{N}$, $2-1 = 1 \in \mathbb{N}$, mas $1-2 = -1 \notin \mathbb{N}$.
- O conjunto $\mathbb{N}$ é fechado em relação à operação de soma.

$\star$

1.2 Relações

Uma **relação** R sobre dois conjuntos A e B é definida como um subconjunto de $A \times B$.

Relações representam abstrações de conceitos matemáticos fundamentais, por exemplo, as operações aritméticas, lógicas e relacionais, além de constituírem a base teórica para o estudo sistemático das funções. O conjunto de todas as relações definíveis sobre $A \times B$ é dado por $2^{A \times B}$.

Exemplo 1.24 A relação $R_1 = \{(a,b) \mid a,b \in \mathbb{N} \text{ e } a > b\}$, sobre $\mathbb{N} \times \mathbb{N}$, contém, entre infinitos outros, os elementos $(2,1), (7,4)$ e $(9,3)$. A relação $R_2 = \{(x,y,z) \mid x,y,z \in \mathbb{Z} \text{ e } x^2 = y^2 + z^2\}$, sobre $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, contém os elementos $(0,0,0)$, $(2,2,0)$, $(2,0,-2)$, $(5,4,3)$, $(-10,8,-6)$ etc. $\star$

Uma relação R aplicada sobre um elemento a de um conjunto A e outro elemento b de um conjunto B pode ser denotada, em notação infixa, por aRb. Se $(a,b) \in R$, diz-se, de forma abreviada, que aRb.

Os conjuntos A e B recebem, respectivamente, os nomes **domínio** e **codomínio** (ou **contradomínio**) da relação R. Por envolver dois conjuntos, essa relação é dita **binária** e seus elementos recebem a designação de **pares ordenados**. Relações binárias sobre um mesmo conjunto A representam subconjuntos de $A \times A$.

Exemplo 1.25 Considere-se a relação binária "$\neq$" sobre o conjunto dos números inteiros. Essa relação se define como o conjunto dos pares ordenados tais que suas duas componentes são diferentes. Alguns dos elementos do conjunto definido por essa relação são $(1,3), (-5,0), (8,-2)$ etc. Utilizando a notação introduzida, os elementos citados, pertencentes a essa relação, são denotados por $1 \neq 3$, $-5 \neq 0$ e $8 \neq -2$, coincidindo, portanto, com a representação tradicional da relação.

Notar que $(1,1), (0,0)$ e $(-5,-5)$ são exemplos de pares ordenados que não satisfazem a essa relação binária, pois suas duas componentes coincidem. $\star$

O conceito de relação pode ser generalizado para mais de dois conjuntos, consistindo, sempre, em subconjuntos definidos sobre o produto cartesiano dos conjuntos participantes da relação. A relação, nesse caso, é dita uma relação "n-ária", e corresponde a um subconjunto do produto cartesiano dos conjuntos envolvidos. Sejam n conjuntos $A_1, A_2, ..., A_n$. Os elementos pertencentes ao conjunto definido por uma relação n-ária sobre $A_1, A_2, ..., A_n$ são, portanto, elementos de $A_1 \times A_2 \times ... \times A_n$, e têm a seguinte forma:

$$(a_1, a_2, a_3, ..., a_n)$$

onde $a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n$.

Tais elementos são denominados **ênuplas ordenadas**. Em casos particulares, como para $n = 2,3,4,5$ etc., as ênuplas recebem nomes especiais, geralmente os ordinais de n: pares, triplas, quádruplas, quíntuplas etc. Quando n é grande, usa-se em geral o nome "n-tupla ordenada". Por exemplo, $(a_1, a_2, ..., a_{10})$ é considerada uma década (ou uma 10-tupla) ordenada.

Uma relação binária R sobre um conjunto A é dita:

- **reflexiva**: se $aRa, \forall a \in A$;
- **simétrica**: se aRb implica $bRa, \forall a, b \in A$;
- **transitiva**: se aRb e bRc implicam $aRc, \forall a, b, c \in A$;

sendo que a, b, c não precisam ser necessariamente distintos.

Exemplo 1.26 A relação "maior ou igual" ($\geq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ é reflexiva, pois $\forall a \in \mathbb{N}, a \geq a$. Já a relação "diferente" ($\neq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ não é reflexiva, pois não é verdade que para $a \in \mathbb{N}, a \neq a$. ⋆

Exemplo 1.27 A relação "diferente" ($\neq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ é simétrica, pois $\forall a, b \in \mathbb{N}, a \neq b \Rightarrow b \neq a$. Já a relação "maior ou igual" ($\geq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ não é simétrica, pois $a \geq b$ não implica necessariamente $b \geq a$. ⋆

Exemplo 1.28 A relação "menor ou igual" ($\leq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ é transitiva, pois $\forall a, b, c \in \mathbb{N}, (a \leq b) \wedge (b \leq c) \Rightarrow a \leq c$. Já a relação "diferente" ($\neq$) definida sobre o conjunto dos números naturais $\mathbb{N}$ não é transitiva, pois $(a \neq b) \wedge (b \neq a)$ não implica $a \neq a$ (notar que neste caso $c = a$). ⋆

Exemplo 1.29 A relação binária "identidade" (=) definida sobre o conjunto dos números inteiros $\mathbb{Z}$ como o conjunto de todos os pares ordenados para os quais as duas componentes são idênticas. Ela é reflexiva, pois $a = a, \forall a \in \mathbb{Z}$; é simétrica, pois $a = b$ implica $b = a, \forall a, b \in \mathbb{Z}$; e transitiva, uma vez que $a = b$ e $b = c$ implica $a = c, \forall a, b, c \in \mathbb{Z}$. Alguns elementos do conjunto definido por essa relação são $(4,4), (0,0), (-7,-7)$ etc. Notar que pares ordenados, como $(1,-3), (0,5)$ e $(7,9)$, não pertencem a essa relação. ⋆

Exemplo 1.30 A relação binária "maior" ($>$), definida como o conjunto dos pares ordenados cujas primeiras componentes tenham valor maior que as segundas componentes, aplicada sobre o mesmo conjunto $\mathbb{Z}$, revela-se não reflexiva, pois não é verdade que $a > a, \forall a \in \mathbb{Z}$; não simétrica, já que $a > b$ não implica $b > a, \forall a$ e $b \in \mathbb{Z}$; porém ela é transitiva, uma vez que $a > b$ e $b > c$ implica $a > c, \forall a, b, c \in \mathbb{Z}$. ⋆

Uma relação que seja simultaneamente reflexiva, simétrica e transitiva é denominada relação de equivalência. Se R é uma **relação de equivalência** sobre um conjunto A, então R estabelece uma partição do conjunto A.

Suponha-se que R seja uma relação de equivalência sobre A, e $A_i, i \geqslant 0$, uma partição de A induzida por R. Então, valem as seguintes propriedades:

- $(a,b) \in R$ se e somente se $\forall i, j, (a \in A_i \wedge b \in A_j) \Rightarrow (i = j)$;
- $(a,b) \notin R$ se e somente se $\forall i, j, (a \in A_i \wedge b \in A_j) \Rightarrow (i \neq j)$.

Teorema 1.4 (Relação binária e partição) "Seja R uma relação binária reflexiva, simétrica e transitiva sobre um conjunto A. Então existe uma partição $P_0, P_1, ..., P_n$ de A tal que (i) se aRb, então $a, b \in P_i$, para algum $0 \leqslant i \leqslant n$; (ii) se $(a,b) \notin R$, então $a \in P_i$ e $b \in P_j$, com $i \neq j$; (iii) todo a pertence a um único conjunto P_i e (iv) a união de todos $P_0, P_1, ..., P_n$ resulta em A."

Para cada $a \in A$, considere o conjunto $classe(a) = \{b \mid aRb\}$. Tais conjuntos recebem o nome de classes de equivalência.

- Primeira parte (i):
  Considere que $(a,b) \in R$, ou seja, aRb. Desejamos provar que $classe(a) = classe(b)$, ou seja, que a e b pertencem ao mesmo conjunto. Para isso, vamos primeiro provar que todo elemento de $classe(a)$ é também elemento de $classe(b)$. Em seguida, provaremos o contrário, ou seja, que todo elemento de $classe(b)$ é também elemento de $classe(a)$.
  Considere um elemento c qualquer, $c \in classe(a)$. Portanto, aRc. Por outro lado, como R é simétrica, segue que bRa. Como ela também é transitiva (pois bRa e aRc), segue que bRc, ou seja, que $c \in class(b)$. Portanto, todo elemento de $classe(a)$ também é elemento de $classe(b)$. Considere agora $c \in classe(b)$. Então, bRc. Pela transitividade de R, temos que aRc (pois aRb e bRc). Logo, $c \in class(a)$ e todo elemento de $classe(b)$ também é elemento de $classe(a)$. Segue que $class(a) = class(b)$ e, portanto, que a e b pertencem à mesma classe de equivalência pois, pela reflexividade, $a \in class(a)$ e $b \in classe(b)$.
- Segunda parte (ii):
  Considere que $(a,b) \notin R$ e suponha que exista um elemento c tal que $c \in class(a)$ e $c \in class(b)$. Logo, aRc e bRc. Pela simetria, temos que cRb e, pela transitividade (aRc e cRb), podemos assumir que aRb. Mas aRb contradiz a hipótese de que $(a,b) \notin R$. Logo, a hipótese é falsa e não pode existir tal c. Ou seja, $class(a) \cap class(b) = \emptyset$ e a e b pertencem à classes de equivalência distintas.
- Terceira parte (iii):
  Como aRa, segue que $a \in class(a)$. Logo, todo elemento a pertence a alguma classe de equivalência. Para provar que essa classe é única, suponha que $a \in c_1$ e $a \in c_2$, com $c_1 \neq c_2$. Conforme o resultado anterior (de que os elementos que satisfazem uma relação devem pertencer ao mesmo conjunto), isso implicaria na falsidade de aRa (onde o primeiro a pertenceria à c_1 e o segundo a pertenceria à c_2), uma vez se trata de elementos de classes distintas (c_1 e c_2). Mas isso contradiz aRa, logo a hipótese é falsa e a não pode pertencer a duas classes diferentes.
- Quarta parte (iv):
  Como todo elemento de A pertence a uma única classe de equivalência, a união de tais classes resulta em A.

□

Exemplo 1.31 Considere-se o conjunto $\mathbb{Z}$ dos números inteiros e a relação binária:

$$\begin{aligned} Q &: \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a^2 = b^2\} \\ Q &= \{(0,0),(1,1),(1,-1),(-1,1),(-1,-1)...(n,n),(n,-n),(-n,n),(-n,-n)...\} \end{aligned}$$

É fácil verificar que Q é reflexiva, simétrica e transitiva. Logo, é uma relação de equivalência. Q induz à partição $\{A_0, A_1, ...\}$ de $\mathbb{Z}$, onde:

$$\begin{aligned} A_0 &= \{0\} \\ A_1 &= \{1,-1\} \\ A_2 &= \{2,-2\} \\ &... \\ A_n &= \{n,-n\} \\ &... \end{aligned}$$

Quaisquer que sejam os números $a,b \in \mathbb{Z}$ considerados, se $(a,b) \in Q$, então a e b pertencem necessariamente ao mesmo conjunto A_i, para algum valor de $i \geqslant 0$. Se $(a,b) \notin Q$, a e b pertencerão sempre a conjuntos distintos dessa partição de $\mathbb{Z}$. ⋆

1.3 Funções

Uma **função** é um mapeamento que associa elementos de um conjunto denominado **domínio** a elementos de um outro conjunto, chamado **codomínio** ou **contradomínio**. Essa associação deve ser tal que cada elemento do domínio esteja associado a no máximo um elemento do conjunto codomínio.

Formalmente, uma função entre um conjunto A (domínio) e um conjunto B (codomínio) é definida como uma relação R entre esses conjuntos, de modo que:

$$\forall (a,b),(a,c) \in R, b = c$$

Portanto, o termo "função" refere-se um tipo particular de relação, em que cada elemento do domínio está associado a, no máximo, um único elemento do codomínio. Em outras palavras, toda função é uma relação, mas nem toda relação é uma função.

Denota-se uma função f entre dois conjuntos X e Y por:

$$f : X \to Y$$

Exemplo 1.32 Considere-se f_1 e f_2 definidas abaixo:

$$\begin{aligned} f_1 &= \{(1,5),(2,3),(4,5),(8,1),(7,3)\} \\ f_2 &= \{(6,7),(9,0),(6,3),(4,3),(3,1)\} \end{aligned}$$

A relação f_1 é aderente à definição de função, ao passo que f_2 é uma relação mas não uma função, devido à presença simultânea dos pares $(6,7)$ e $(6,3)$, que associam o mesmo elemento 6 do domínio a dois elementos distintos do codomínio (7 e 3). As Figuras 1.4 e 1.5 ilustram, respectivamente, as relações f_1 e f_2. ⋆

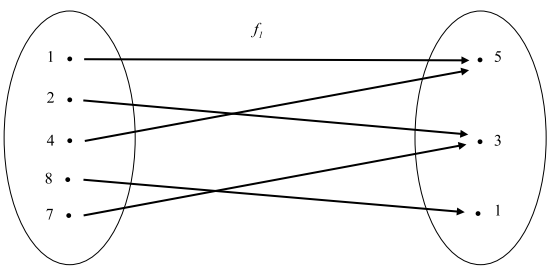


Figura 1.4 Relação que é também função.

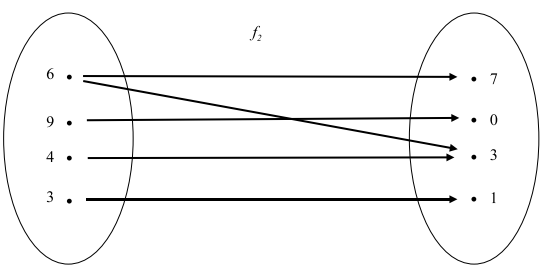


Figura 1.5 Relação que não é função.

A associação estabelecida pela função f entre um elemento x do conjunto domínio X com um elemento y do conjunto codomínio Y é denotada por $f(x) = y$. De maneira equivalente, diz-se que $(x, y) \in f$.

O **conjunto imagem** de f, denotado por I_f, é o conjunto formado por todos os elementos do codomínio Y que estejam em correspondência com elementos de X, ou seja, $I_f \subseteq Y$. Formalmente,

$$I_f = \{y \in Y \mid y = f(x)\}$$

O elemento x é denominado **argumento** da função f, e y é denominado **imagem** de x pela **aplicação** de f. Funções com múltiplos argumentos são definidas como um mapeamento em que o conjunto domínio corresponde ao produto cartesiano de múltiplos conjuntos:

$$f : X_1 \times X_2 \times ... \times X_n \rightarrow Y$$

Funções com um, dois ou três argumentos são, respectivamente, denominadas funções unárias, binárias ou ternárias, e assim por diante.

Diz-se também que uma função que associa pares ordenados sobre um conjunto X, ou seja, elementos de X^2 com elementos do próprio conjunto X, é uma **função (operação) binária** sobre X.

Exemplo 1.33 Considere $f_1 : \mathbb{N} \rightarrow \mathbb{N}, f_1 = \{y \in \mathbb{N} \mid y = x^3, x \in \mathbb{N}\}$. A função f_1 é unária, pois associa cada elemento de $\mathbb{N}$ ao seu cubo. Portanto, $f_1 : \mathbb{N} \rightarrow \mathbb{N}$. Alguns dos infinitos elementos do conjunto definido por f_1 são: $(1,1), (2,8), (3,27)$ etc. Denota-se $f_1(2) = 8$, ou ainda $(2,8) \in f_1$. ⋆

Exemplo 1.34 Seja $f_2 : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, f_2 = \{z \in \mathbb{Z} \mid z = x + y; x, y \in \mathbb{Z}\}$. A função binária f_2 define a operação (função) de adição sobre o conjunto dos números inteiros $\mathbb{Z}$, sendo elementos de f_2 : $((1,2),3), ((-3,7),4), ((0,5),5)$ etc. Escreve-se $f_2(-3,7) = 4$, ou ainda $((-3,7),4) \in f_2$. ⋆

Uma função se diz uma **função total** (denotada pelo símbolo "$\rightarrow$") quando especifica associações para todos os elementos do conjunto domínio, sem exceção. Formalmente:

$$\forall x \in X, \exists y \in Y \mid y = f(x)$$

Exemplo 1.35 A Figura 1.6 ilustra o conceito de função total. Notar que todos os elementos de X têm correspondência com algum elemento de Y. ⋆

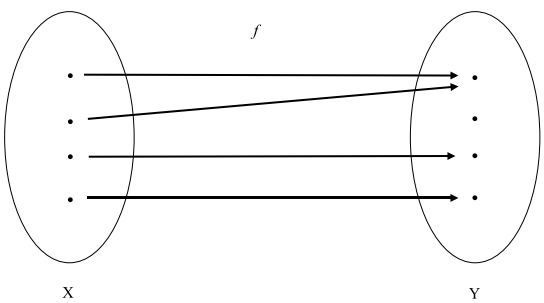


Figura 1.6 Função total.

Exemplo 1.36 Sejam $X = \{0,1,2\}$ e $Y = \{a,b,c\}$, respectivamente, o conjunto domínio e o conjunto codomínio da função $f_1 = \{(0,a), (1,b), (2,a)\}$. A função $f_1 : X \rightarrow Y$ é total, pois todos os elementos do conjunto domínio estão em correspondência com algum elemento do conjunto codomínio. Nesse caso, o conjunto imagem de f_1 é $\{a,b\}$. ⋆

Quando uma função não é definida para todos os elementos de seu domínio, ela recebe a denominação de **função parcial** (denotada pelo símbolo "$\nrightarrow$"). Formalmente:

$$\exists x \in X \mid f(x) \text{ não é definida}$$

Exemplo 1.37 A Figura 1.7 ilustra o conceito de função parcial. Notar a existência de um elemento de X sem correspondente em Y. ⋆

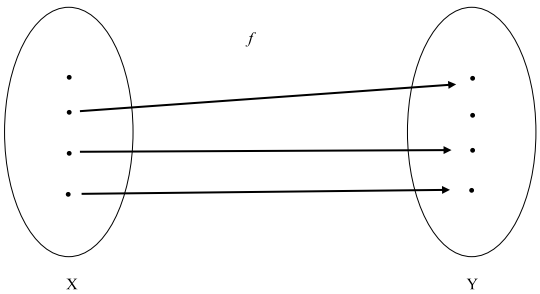


Figura 1.7 Função parcial.

Exemplo 1.38 Seja $X = \{0,1,2\}, Y = \{a,b,c\}$ e $f_2 = \{(0,b),(2,b)\}$. A função $f_2 : X \nrightarrow Y$ é parcial, pois não há associação do elemento "1" pertencente ao conjunto domínio a qualquer elemento do conjunto codomínio. O conjunto imagem para essa função é $\{b\}$. ⋆

Diz-se que uma função é **um-para-um**, ou simplesmente uma função **injetora**, quando elementos distintos do domínio X estiverem associados a elementos distintos do codomínio Y, ou seja, quando não houver quaisquer dois elementos distintos do conjunto domínio associados ao mesmo elemento do conjunto imagem:

$$\forall x_1, x_2 \in X, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

De maneira equivalente, uma função é dita **injetora** se cada elemento do conjunto codomínio estiver associado a, no máximo, um elemento do conjunto domínio.

As Figuras 1.6 e 1.7 representam funções que são, respectivamente, não injetora e injetora.

Exemplo 1.39 Seja $X = \{0,1,2\}, Y = \{a,b,c\}$ e $f_3 = \{(0,c),(1,b)\}$. A função $f_3 : X \to Y$ é injetora, pois não existe um mesmo elemento de Y associado a mais de um elemento de X. Por outro lado, a função f_2, definida no Exemplo 1.38, é parcial mas não injetora, pois o elemento b de seu conjunto imagem está simultaneamente associado aos elementos 0 e 2 do conjunto domínio. ⋆

Uma função f é dita **sobrejetora** se todos os elementos do conjunto codomínio estiverem associados a elementos do conjunto domínio, ou seja, se I_f, o conjunto imagem de f, for igual ao conjunto codomínio de f:

$$\forall y \in Y, \exists x \in X \mid y = f(x)$$

Dito de outra forma, uma função é sobrejetora se todo elemento do conjunto codomínio estiver associado a pelo menos um elemento do conjunto domínio.

Exemplo 1.40 As funções das Figuras 1.6 e 1.7 não são sobrejetoras. A Figura 1.8 ilustra uma função sobrejetora. Não há elemento de Y que não corresponda a algum elemento de X. ⋆

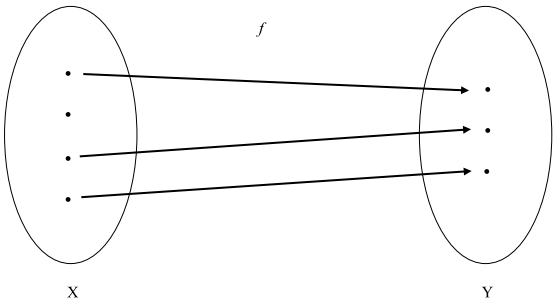


Figura 1.8 Função sobrejetora.

Exemplo 1.41 Seja $X = \{0,1,2\}, Y = \{a,b,c\}$ e $f_4 = \{(0,c),(1,b),(2,a)\}$. A função $f_4 : X \to Y$ é sobrejetora, pois $Y = I_f = \{a,b,c\}$. Em adição, pode-se observar que f_4 é simultaneamente uma função total, injetora e sobrejetora, e também que as funções f_1 (Exemplo 1.36), f_2 (Exemplo 1.38) e f_3 (Exemplo 1.39) anteriormente definidas não são sobrejetoras. ⋆

Uma função que seja simultaneamente total, injetora e sobrejetora recebe a denominação de função **bijetora**.

Exemplo 1.42 As funções das Figuras 1.6, 1.7 e 1.8 não são bijetoras. Em particular, a da Figura 1.6 é total, não injetora e não sobrejetora; a da Figura 1.7 é parcial, injetora e não sobrejetora; e a da Figura 1.8 é parcial, injetora e sobrejetora. A Figura 1.9 ilustra uma função bijetora. Há uma correspondência biunívoca entre os elementos de X e os de Y. ⋆

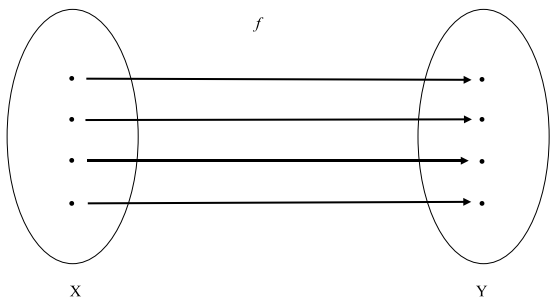


Figura 1.9 Função bijetora.

Exemplo 1.43 Seja $f_5 = \{(0,a),(1,b),(2,c)\}$. A função $f_5 : X \to Y$, assim como a função f_4 definida no Exemplo 1.41, é bijetora. As funções f_1 (Exemplo 1.36), f_2 (Exemplo 1.38) e f_3 (Exemplo 1.39) não são bijetoras. ⋆

Exemplo 1.44 Considerem-se as funções adição, sobre o conjunto dos números naturais, divisão, sobre o conjunto dos números reais, e raiz quadrada, sobre o conjunto dos números inteiros:

- $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Ela não é injetora, pois a soma de dois números naturais quaisquer pode corresponder à soma de outros números naturais distintos (por exemplo, ((3,4),7) e ((5,2),7)). É sobrejetora, pois todo número natural pode ser expresso como a soma de dois outros números naturais. É total, pois a cada par de números naturais sempre corresponde um outro número natural.
- $/ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$. Não é injetora, pois existem vários casos em que a divisão de dois números reais corresponde ao mesmo número real (por exemplo, os casos ((10.0,2.5),4.0) e

((20.0,5.0),4.0)). É sobrejetora, pois todos os números reais podem ser expressos como a divisão de dois outros números reais (por exemplo, todos os casos ((x,1.0),x)). Não é total, pois a divisão não é definida quando o denominador é zero (por exemplo, ((1,0),?)).[1]

- $\sqrt{}: \mathbb{Z} \to \mathbb{Z}$. É injetora, pois não é possível que dois números inteiros diferentes tenham a mesma raiz inteira ((4,2), (9,3) e (3,?)). Não é sobrejetora, pois nem todo número inteiro corresponde à raiz quadrada de algum outro número inteiro (por exemplo, (?,-3). Não é total, pois a operação raiz quadrada não é definida para números inteiros negativos (por exemplo, (-2,?)).

A Tabela 1.1 resume esses resultados. ⋆

Tabela 1.1 Propriedades das funções $+, /$ e $\sqrt{}$

	Injetora?	Sobrejetora?	Total?
$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$	Não	Sim	Sim
$/ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$	Não	Sim	Não
$\sqrt{} : \mathbb{Z} \to \mathbb{Z}$	Sim	Não	Não

A igualdade de funções pode ser definida a partir de duas perspectivas distintas. A perspectiva **extensional** determina que duas funções são iguais se elas produzem os mesmos resultados para as mesmas entradas, independente da forma como as saídas são geradas. A perspectiva **intencional** determina que duas funções são iguais se elas produzem os mesmos resultados para as mesmas entradas da mesma forma. A matemática costuma adotar a perspectiva extensional, já a computação costuma adotar a perspectiva intencional.

Considere, por exemplo, duas funções f (recursiva) e g (iterativa) que produzem o fatorial de um número natural. Do ponto de vista da matemática (extensional) as funções são idênticas. Do ponto de vista da computação (intencional) elas são distintas, já que produzem as suas saídas de forma diferente (f é recursiva e g é iterativa). Por isso, é sempre bom considerar que tipo de perspectiva está sendo considerada para se determinar a igualdade de funções.

1.4 Grafos

Um **grafo** é um par ordenado (V,A), em que V denota o conjunto de **vértices** (ou nós) do grafo e A denota uma relação binária sobre V, através da qual são especificados os **arcos** do grafo. Os arcos indicam associações entre os vértices do grafo. Dois vértices $v_i, v_j \in V$ tais que $(v_i, v_j) \in A$ são ditos vértices **adjacentes**.

A estrutura de um grafo pode ser mais bem entendida com o auxílio de uma representação gráfica. Nesse caso, os nós são denotados por círculos e os arcos por linhas que unem pares de vértices.

Exemplo 1.45 Sejam G_1, V_1 e A_1 conforme a seguir:

$$\begin{aligned} G_1 &= (V_1, A_1) \\ V_1 &= \{0,1,2,3\} \end{aligned}$$

[1] O símbolo "." é usado em substituição ao símbolo ",", na representação de números reais neste exemplo, para evitar ambiguidade de interpretação com a vírgula que separa os elementos de um par ordenado.

$$A_1 \quad = \quad \{(0,1),(0,2),(0,3),(1,3),(2,3)\}$$

O grafo G_1 possui quatro vértices, respectivamente numerados de 0 a 3, e cinco arcos, que conectam pares de vértices, conforme especificado em A_1. Graficamente, G_1 pode ser ilustrado conforme a Figura 1.10. ⋆

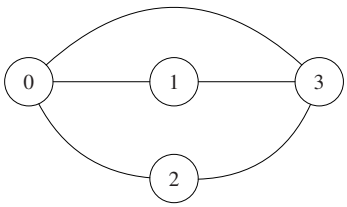


Figura 1.10 Grafo não orientado G_1.

Diz-se que um grafo é **orientado** quando os pares da relação binária A sobre V forem ordenados, ou seja, quando houver relação de ordem entre os elementos que formam os pares $(v_i, v_j) \in A$. Caso contrário, diz-se que o grafo é **não orientado**.

Na prática, costuma-se convencionar que v_i **precede** v_j no par $(v_i, v_j) \in A$. Nesse caso, v_i é denominado **predecessor** de v_j. Por outro lado, v_j **sucede** v_i nesse mesmo par, e por isso é denominado **sucessor** de v_i. Diz-se também que o arco (v_i, v_j) **emerge** do vértice v_i (ou ainda "se inicia no", "parte do") e **atinge** o vértice v_j (ou "termina no", "chega ao", "alcança").

Grafos orientados empregam, em sua representação, setas associadas aos arcos, denotando, através do sentido dos arcos do grafo, a relação de ordem existente entre os nós unidos pelo arco em questão. A omissão das setas, em grafos não orientados, equivale a considerar que todos os arcos representam conexões bidirecionais.

Exemplo 1.46 No Exemplo 1.45 o grafo G_1 é representado como um grafo não orientado. Considerando-se desta vez o grafo G_1 como sendo um grafo orientado, e sem alterar qualquer aspecto de sua definição formal, ele poderia ser representado graficamente conforme a Figura 1.11. ⋆

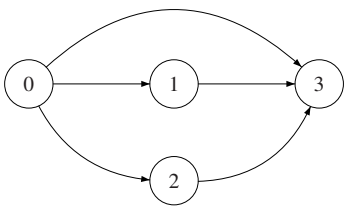


Figura 1.11 Grafo orientado G_1.

Um grafo orientado é dito **ordenado** quando houver uma relação de ordem pré-convencionada sobre todos os arcos que emergem dos diversos vértices do grafo. Essa relação de ordem tem por objetivo estabelecer uma sequência entre os diversos arcos que partem de um mesmo vértice, e não costuma ser definida explicitamente, uma vez que conjuntos não incorporam o conceito de sequência.

Quando se deseja ordenar os arcos que emergem de cada vértice, é comum que se leve em conta como referência a sequência em que os arcos comparecem na representação algébrica da função A. Eventualmente pode-se considerar uma sequência diferente, desde que devidamente explicitada na representação do grafo.

Exemplo 1.47 Sejam:

$$\begin{aligned} G_2 &= (V_2, A_2) \\ V_2 &= \{a,b,c,d\} \\ A_2 &= \{(a,b),(b,a),(a,c),(a,d),(c,b),(d,c),(c,d)\} \end{aligned}$$

Suponha-se, para efeito didático, que A_2 fosse constituída de uma sequência de pares ordenados (e não de um conjunto de pares ordenados), redigida de maneira análoga à representação do conjunto, porém sem as chaves:

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

Suponha-se, ainda, que um mesmo par ordenado não figure mais de uma vez na mesma sequência, e que exista uma relação de ordem implícita entre os pares ordenados, de tal forma que $(a,b) < (b,a) < (a,c) < ... < (c,d)$. Isso facilita a percepção de uma relação de ordem definida para os arcos de G_2, conforme mostrado a seguir:

- Vértice a: inicialmente (a,b), depois (a,c) e por último (a,d)
- Vértice b: apenas (b,a)
- Vértice c: primeiro (c,b) depois (c,d)
- Vértice d: apenas (d,c)

Essa ordenação pode ser representada graficamente numerando-se os arcos do grafo, indicando-se assim a ordenação relativa dos arcos que partem de um mesmo vértice: ⋆

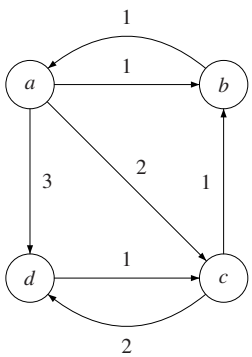


Figura 1.12 Grafo ordenado G_2.

Três importantes conceitos estão relacionados a grafos orientados, sejam eles ordenados ou não. O número N_S de **ramificações de saída** (ou *fan-out*) de um dado vértice de um grafo orientado indica a quantidade de arcos que partem dele. De modo similar, o número N_E de **ramificações de entrada** (ou *fan-in*) de um determinado vértice refere-se à quantidade de arcos do grafo que possuem o vértice em questão como destino. Vértices com $N_E = 0$ são denominados **vértices-base** ou **vértices-raiz**, e vértices com $N_S = 0$ são denominados **vértices-folha**.

Um **caminho** entre dois arcos, respectivamente denominados arcos **inicial** e **final**, em um grafo, é uma sequência ordenada de arcos, de tal forma que o vértice predecessor de cada arco, à exceção do arco inicial, corresponde ao vértice sucessor do arco imediatamente anterior na sequência ordenada.

O **comprimento** de um caminho é o número de arcos que o formam. Por definição, um caminho de comprimento zero é aquele que inicia e termina no mesmo vértice sem percorrer nenhum arco.

Um caminho é denominado **ciclo** se o vértice predecessor do primeiro arco coincidir com o vértice sucessor do último arco que o define. Grafos orientados que possuem pelo menos um ciclo são ditos grafos **cíclicos**. Caso contrário, são denominados grafos **acíclicos**.

Exemplo 1.48 Para o grafo G_2 da Figura 1.12 (Exemplo 1.47):

$$N_S(a) = 3, N_S(b) = 1, N_S(c) = 2, N_S(d) = 1$$
$$N_E(a) = 1, N_E(b) = 2, N_E(c) = 2, N_E(d) = 2$$

A sequência $(a,c)(c,b)$ constitui um caminho, pois o vértice predecessor do segundo arco (c em (c,b)) é idêntico ao vértice sucessor do arco anterior (c em (a,c)), e seu comprimento é 2. A sequência $(a,d)(c,d)(d,c)$ não constitui um caminho, pois o vértice predecessor do segundo arco ((c)) é diferente do vértice sucessor do arco anterior ((d)). O grafo G_2 é do tipo cíclico, pois é possível identificar inúmeros ciclos, dentre os quais $(a,b)(b,a)$ ou $(a,d)(d,c)(c,d)(d,c)(c,b)(b,a)$. ⋆

Muitas vezes pode ser útil associar aos vértices de um grafo, aos arcos de um grafo ou, eventualmente, a ambos rótulos que representem informação adicional para a sua interpretação. Nesses casos, diz-se que o grafo é **rotulado**. Conforme o caso, caracteriza-se a rotulação de vértices ou então a rotulação de arcos do grafo.

Uma **rotulação de vértices** é definida como sendo uma função f_V que associa os elementos de V a elementos de um conjunto R_V, denominado alfabeto de rotulação de vértices. De modo análogo, uma **rotulação de arcos** é realizada através de uma função f_A que associa elementos de A a elementos de um conjunto R_A, denominado alfabeto de rotulação de arcos.

Exemplo 1.49 Sejam:

$$\begin{aligned} G_3 &= (V_3, A_3) \\ V_3 &= \{0,1,2\} \\ A_3 &= \{(0,1),(1,2),(0,2)\} \end{aligned}$$

Uma possível rotulação simultânea de vértices e arcos em G_3 seria:

- $f_V = \{(0,\Phi),(1,\Gamma),(2,\Psi)\}$, com $R_V = \{\Phi,\Gamma,\Psi\}$
- $f_A = \{((0,1),\phi),((1,2),\gamma),((0,2),\psi)\}$, com $R_A = \{\phi,\gamma,\psi\}$

Esquematicamente, essa rotulação pode ser representada conforme mostra a Figura 1.13. ⋆

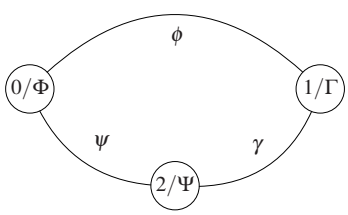
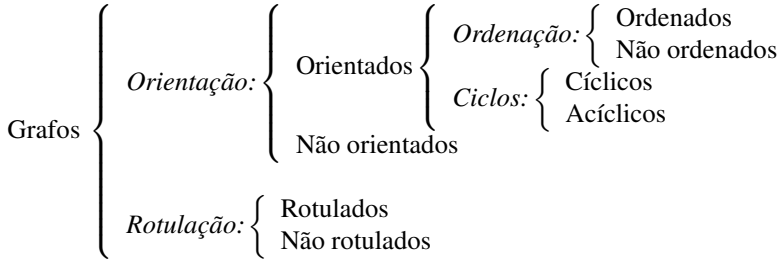


Figura 1.13 Grafo rotulado G_3.

Quanto à sua natureza, os grafos podem ser classificados em grafos orientados ou grafos não orientados, e também em grafos rotulados ou grafos não rotulados. Os grafos orientados

podem ainda ser classificados em grafos ordenados ou grafos não ordenados, e ainda como grafos cíclicos ou grafos acíclicos:



1.5 Árvores

São especialmente importantes, no estudo das linguagens formais, e muito aplicados na prática, para a análise e construção de compiladores, os grafos acíclicos orientados e as árvores. Estas, por sua vez, constituem um caso particular dos grafos acíclicos orientados ordenados.

Uma árvore ordenada, ou simplesmente uma **árvore**, é um grafo acíclico orientado e ordenado que possui as seguintes características adicionais:

- Há apenas um vértice r tal que $N_E(r) = 0$. Esse vértice diferenciado é denominado **raiz** da árvore.
- Todos os demais vértices possuem $N_E = 1$.
- Para cada vértice há sempre um único caminho que o liga à raiz da árvore.

Para vértices a e b que fazem parte de um mesmo caminho em uma árvore, diz-se que a é **ancestral** de b se for possível atingir b a partir de a. Nesse caso, b é dito **descendente** de a. Quando entre a e b não houver nenhum vértice intermediário, diz-se que a e b são adjacentes. Nessa situação, diz-se ainda que o vértice a é ancestral direto, ou **pai**, do vértice b, e que este é descendente direto, ou **filho**, do vértice a. O ancestral mínimo comum de dois vértices a e b corresponde ao (único) antecessor de ambos que seja também descendente de todos os antecessores comuns de a e b.

Vértices tais que $N_S = 0$ são denominados **folhas** da árvore. Os demais são denominados **vértices internos**. Inclui-se, por essa definição, entre os vértices internos de uma árvore, o vértice-raiz dessa árvore.

A **profundidade** de um vértice em uma árvore é o comprimento do caminho iniciado em sua raiz, e que termina no referido vértice. A profundidade de uma árvore (também conhecida como **altura** da árvore) é definida como sendo a maior dentre as profundidades de seus vértices.

A **fronteira** de uma árvore é a sequência formada pelos rótulos dos vértices-folha, quando são colhidos de cima para baixo e da esquerda para a direita.

Árvores costumam ser representadas esquematicamente com a raiz na parte superior da figura e com os arcos e demais vértices "crescendo" para baixo. Normalmente, as representações esquemáticas das árvores não incorporam indicações sobre a orientação e a ordenação dos arcos, as quais neste caso se tornam implícitas, podendo ser inferidas a partir da própria figura, de acordo com as seguintes convenções, usualmente adotadas: todos os arcos "apontam" para baixo e são implicitamente ordenados da esquerda para a direita.

Uma árvore é dita **binária** se cada vértice-pai possuir no máximo dois vértices-filho. Árvores binárias são casos particulares de árvores gerais e são úteis na demonstração de certos teoremas.

Exemplo 1.50 Considere-se a árvore da Figura 1.14. Neste exemplo, o vértice V_1 é ancestral direto (pai) de V_{11}. Este, por sua vez é descendente direto (filho) de V_1. O vértice "Raiz" é ancestral de V_{00} e o vértice V_{01} é descendente de "Raiz". "Raiz" é também o mínimo ancestral comum dos vértices V_{00} e V_{11}, que, por sua vez, são folhas dessa árvore e apresentam profundidade igual a 2. V_0 e V_1 são vértices internos, e possuem profundidade 1. A profundidade (ou altura) desta árvore é igual a 2. A fronteira desta árvore é a sequência $V_{00}V_{01}V_{10}V_{11}$. ⋆

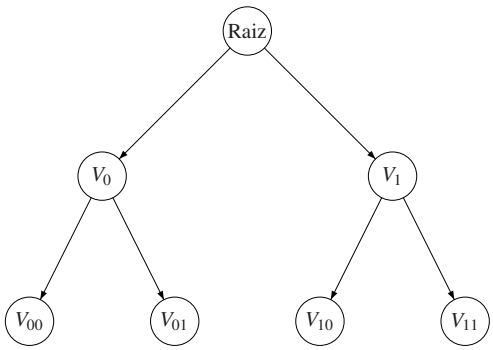


Figura 1.14 Árvore para o Exemplo 1.50.

1.6 Lógica formal

Considerada por alguns como os fundamentos da matemática e por outros como um ramo da matemática propriamente dita, a **lógica formal** se ocupa da representação e validação de argumentações (ou **proposições**). A lógica formal se apresenta de diversas formas, como a lógica proposicional (cujas sentenças são constituídas apenas por variáveis agrupadas em torno de um conjunto pequeno de conectivos) e a lógica de predicados (também conhecida como lógica de primeira ordem), que estende a lógica proposicional com o uso dos quantificadores universal e existencial, além de predicados (funções aplicadas sobre os objetos do enunciado em questão e que produzem valores lógicos como resultado).

O estudo de linguagens formais, assim como da computação, da matemática e de qualquer teoria, de uma forma geral, envolve uma coleção (geralmente restrita) de definições e uma coleção (geralmente extensa) de propriedades que são verificadas por essas definições. A Teoria das Linguagens Formais, por exemplo, é praticamente toda construída em torno de uma única definição: a definição de gramática. A partir dessa definição, existem dezenas de propriedades que podem ser enunciadas e provadas.

O enunciado de uma propriedade é uma afirmação de que aquela propriedade é válida num contexto de determinadas premissas. Todo enunciado precisa ser provado para ser aceito como verdadeiro, e a prova pode ou não ser trivial. Quando a prova não é trivial, isso caracteriza o que se chama de **teorema**. Um **lema** é um enunciado cuja prova é, normalmente, um pouco menos complexa do que a prova de um teorema. Geralmente os lemas são auxiliares na prova de teoremas. Um **corolário** é um enunciado que deriva, de forma trivial, de um teorema ou lema provado anteriormente.

Diferentes técnicas podem ser usadas para se obter a prova de que uma propriedade é válida (ver Seção 1.7). Na presente seção, estudamos a linguagem que é usada para escrever tais enunciados (inicialmente a lógica proposicional e depois a lógica de predicados). O objetivo aqui não é fazer um estudo aprofundado do assunto (para isso, recomenda-se [3]), mas apenas introduzir a notação e a terminologia que serão usadas no restante do texto.

Uma lógica é necessária, portanto, para escrever o enunciado de teoremas e lemas de forma concisa, precisa e não ambígua. Nesse caso, tais enunciados ou propriedades são chamados de **proposições**. A lógica de predicados é uma das mais usadas para essa finalidade, por causa de várias das suas características, como simplicidade, expressividade e uso geral, além de ser uma escolha natural para a expressão de proposições gerais, semelhante à que usamos no nosso dia a dia. Assim, o objetivo desta seção é introduzir a sintaxe e a semântica da lógica de predicados, mostrando como é possível construir e interpretar proposições (sentenças) dessa linguagem.

A **lógica proposicional** é uma lógica mais simples do que a **lógica de predicados** e será apresentada antes, como uma preparação para esta última. Uma proposição dessa lógica é uma fórmula que usa variáveis e conectivos lógicos, sendo o emprego deles regido por uma gramática bastante simples (ver Seção 2.3).

$$
\begin{array}{lcl}
\text{fórmula} & ::= & \text{variável} \\
& | & \bot \\
& | & \top \\
& | & (\text{fórmula} \wedge \text{fórmula}) \\
& | & (\text{fórmula} \vee \text{fórmula}) \\
& | & (\text{fórmula} \Rightarrow \text{fórmula}) \\
& | & (\text{fórmula} \Leftrightarrow \text{fórmula}) \\
& | & (\neg\ \text{fórmula}) \\
\text{variável} & ::= & a \mid b \mid c \mid \ldots
\end{array}
$$

Os conectivos lógicos são os seguintes:

- $\wedge$: Conjunção ("e");
- $\vee$: Disjunção ("ou");
- $\Rightarrow$: Implicação ("se-então");
- $\Leftrightarrow$: Bi-implicação ($(a \Leftrightarrow b) \equiv (a \Rightarrow b) \wedge (b \Rightarrow a)$) ("se-e-somente-se");
- $\neg$: Negação ($\neg\ a \equiv a \Rightarrow \bot$) ("não"); eventualmente, um traço na parte de cima de uma fórmula é usado para representar a negação dela ($\neg x \equiv \overline{x}$).

A lógica proposicional também utiliza os seguintes símbolos que representam, respectivamente, a proposição falsa e a proposição verdadeira:

- $\bot$: Falso;
- $\top$: Verdadeiro ($\top \equiv \bot \Rightarrow \bot$).

Se não existem dúvidas sobre a sintaxe de uma proposição, o mesmo não se pode dizer acerca do seu significado. A semântica associada aos conectivos, e às fórmulas de uma maneira geral, não é única. Na sequência, apresentaremos duas das interpretações mais comuns: Tarski e BHK.

A interpreptação tradicional (devida a Tarski) associa cada variável a um possível valor (Falso ou Verdadeiro), e procede com a inferência do valor lógico da fórmula completa por meio da aplicação das **tabelas-verdade** dos conectivos. As Tabelas 1.2 até 1.6 a seguir apresentam a tabela-verdade para cada um dos conectivos.

Tabela 1.2 Tabela-verdade para a Conjunção

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

Tabela 1.3 Tabela-verdade para a Disjunção

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

Tabela 1.4 Tabela-verdade para a Implicação

p	q	$p \Rightarrow q$
F	F	V
F	V	V
V	F	F
V	V	V

Na interpretação de Tarski, por exemplo, se a é verdadeiro e b é verdadeiro, então $a \wedge b$ também é verdadeiro.

Em geral, uma fórmula da lógica proposicional é considerada verdadeira quando todas as combinação de valores atribuídos aos seus argumentos (variáveis) resultam em verdadeiro após avaliação feita com o uso das tabelas-verdade dos seus respectivos conectivos.

Exemplo 1.51 A fórmula $a \wedge b \Leftrightarrow b \wedge a$ (que expressa a comutatividade da conjunção $\wedge$) pode ser provada verdadeira considerando-se todas as possibilidades de valores que podem ser atribuídos tanto à variável a quanto à variável b, conforme a Tabela 1.7. ⋆

Exemplo 1.52 São exemplos de fórmulas da lógica proposicional:

- $(a \Rightarrow (b \Rightarrow c)) \Rightarrow (b \Rightarrow (a \Rightarrow c))$
- $(a \wedge b) \Rightarrow (b \wedge a)$
- $(a \vee (a \wedge b)) \Rightarrow a$
- $(a \Rightarrow b) \Rightarrow (\neg\, b \Rightarrow \neg\, a)$

⋆

Tabela 1.5 Tabela-verdade para a Bi-implicação

p	q	$p \Leftrightarrow q$
F	F	V
F	V	F
V	F	F
V	V	V

Tabela 1.6 Tabela-verdade para a Negação

p	q	$p \Leftrightarrow q$
F	F	V
F	V	F
V	F	F
V	V	V

Tabela 1.7 Prova de $a \wedge b \Leftrightarrow b \wedge a$

a	b	$a \wedge b$	$b \wedge a$	$a \wedge b \Leftrightarrow b \wedge a$
$\top$	$\top$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\top$

Uma proposição que é verdadeira para qualquer interpretação (ou atribuição de valores às suas variáveis, na interpretação de Tarski) é denominada uma **tautologia**. Naturalmente, o nosso objetivo é provar que todos os enunciados (expressos como proposições que representam teoremas e lemas) sejam tautologias, para assim formar uma teoria.

Uma interpretação diferente considera que uma fórmula é verdadeira apenas se for possível apresentar uma prova disso (na interpretação BHK). Por exemplo, $a \wedge b$ seria considerada verdadeira, na interpretação BHK, apenas se for possível apresentar provas de que tanto a quando b são verdadeiros. Essa interpretação, usada em conjunto com a chamada **lógica construtiva** (ou intuicionística) (na qual a lei do terceiro excluído — $\forall x, x \vee \overline{x}$ — e suas variações não são consideradas) é a base de muitos provadores de teoremas (ou assistentes de provas), como são chamados os programas de computador que auxiliam na prova de teoremas. A lógica que faz uso da lei do terceiro excluído (ou se suas variantes) é chamada de **lógica clássica**.

Quando a lógica proposicional é estendida com **quantificadores** e também com **predicados**, ela passa a se chamar **lógica de predicados**. Ela é definida por meio da seguinte gramática:

$$
\begin{array}{lcl}
\text{fórmula} & ::= & \text{variável} \\
& | & \bot \\
& | & \top \\
& | & \text{pred\_nome (arg\_list)}
\end{array}
$$

$$
\begin{array}{rl}
| & (\text{fórmula} \wedge \text{fórmula}) \\
| & (\text{fórmula} \vee \text{fórmula}) \\
| & (\text{fórmula} \Rightarrow \text{fórmula}) \\
| & (\text{fórmula} \Leftrightarrow \text{fórmula}) \\
| & (\neg \text{ fórmula}) \\
| & (\forall \text{ variável . fórmula}) \\
| & (\exists \text{ variável . fórmula})
\end{array}
$$

$$
\begin{array}{rcl}
\text{pred\_nome} & ::= & P_0 \mid P_1 \mid P_2 \mid ... \\
\text{arg\_list} & ::= & \text{termo} \mid \text{arg\_list , termo} \\
\text{termo} & ::= & \text{fun\_nome (arg\_list)} \mid \text{variável} \mid \text{constante} \\
\text{fun\_nome} & ::= & f_0 \mid f_1 \mid f_2 \mid ... \\
\text{variável} & ::= & a \mid b \mid c \mid ... \\
\text{constante} & ::= & c_0 \mid c_1 \mid c_2 \mid ...
\end{array}
$$

Os quantificadores:

- $\forall$: Universal ("para todo");
- $\exists$: Existencial ("existe").

são peças-chave na caracterização da lógica de predicados, uma vez que eles possibilitam o raciocínio sobre coleções de elementos. O quantificador universal, por exemplo, é usado para fazer asserções sobre uma coleção (eventualmente infinita) de valores. Por exemplo, $\forall x . x + 0 = x$. O quantificador existencial, por outro lado, é útil quando se deseja mostrar que alguma propriedade é válida para algum valor de uma variável, entre uma coleção (geralmente maior) de valores possíveis. Por exemplo, $\exists y . y^2 = 4$.

A introdução desses quantificadores cria as noções de variáveis "ligadas" e variáveis "livres". Em geral, uma variável ligada é uma variável que está no "escopo" de um nome imediatamente à direita de algum quantificador. Uma variável livre, por sua vez, é uma variável que não é ligada. Por exemplo, x é ligado em $\forall x . x + 0 = x$ e y é livre em $\forall x . (x = y) \Rightarrow (y = x)$. As noções de escopo, variável livre e variável ligada, assim como métodos para determiná-los, podem ser encontrados em qualquer livro introdutório de lógica.

Um **predicado** é uma função que recebe um certo número de argumentos e retorna uma proposição (cujo valor pode ser falso ou verdadeiro). Predicados são usados para definir as propriedades que são compartilhadas por objetos de uma mesma natureza. Por exemplo, o predicado *primo n* pode ser usado para estabelecer que *n* é um número primo, como em *primo 5*. Naturalmente, existem muitos outros números primos, e a cada um deles corresponde uma proposição que pode ser obtida a partir desse predicado (*primo 2*, *primo 3* etc). Um predicado, também chamado de "proposição parametrizada", representa, portanto, uma família de proposições.

Na gramática apresentada, "variável" representa variáveis lógicas, "pred_nome" representa diferentes nomes de predicados e "arg_list" representa uma lista of argumentos (também chamados de "termos") que são usados na chamada de funções ou na formação de predicados. Um termo pode conter chamadas de função aninhadas, assim como variáveis e constantes, representados respectivamente por "variavel" e "constante".

Exemplo 1.53 São exemplos de fórmulas da lógica de predicados:

- $\forall ab.(a \wedge b) \Rightarrow (b \wedge a)$
- $\forall x.x \neq 0 \Rightarrow \exists y.x * y = 1$
- $\forall x.R(x,x) \Rightarrow \forall x.\exists y.R(x,y)$
- $\forall x.R(f(x),g(f(x))) \Rightarrow \forall x.\exists y.R(f(x),y)$

$\star$

Tendo visto a lógica proposicional e também a lógica de predicados, já é possível ler e escrever os enunciados redigidos nessas linguagens e, portanto, entender o significado de proposições que representam lemas e teoremas. O próximo passo é construir as provas deles, e para isso a Seção 1.7 apresenta algumas técnicas. Aqueles que desejarem ir além deverão estudar a Dedução Natural, o Cálculo Lambda e a Teoria das Provas.

1.7 Teoremas e demonstrações

Linguagens formais e autômatos constituem sistemas matemáticos formais, nos quais inúmeras propriedades, em geral formuladas como **teoremas**, podem ser inferidas a partir de verdades previamente conhecidas ou admitidas por hipótese, por intermédio de raciocínios lógicos expressos como **demonstrações**. Tais propriedades sintetizam grande parte dos resultados mais importantes da teoria na área e são fundamentais para o aprendizado e a aplicação do conhecimento adquirido.

A demonstração de teoremas sobre um dado conjunto geralmente exige a prova formal de que uma certa propriedade é satisfeita por todos os membros desse conjunto. Quando se trata de conjuntos com uma quantidade reduzida de elementos, é possível realizar demonstrações particulares para cada elemento individual desse conjunto (que às vezes se reduzem a simples verificações), garantindo assim que a propriedade seja válida para todos os elementos do conjunto.

Há, no entanto, uma óbvia dificuldade prática na aplicação dessa técnica para conjuntos finitos com cardinalidades elevadas. Além disso, esse método exaustivo de demonstração evidentemente não se aplica a conjuntos infinitos.

Para tais casos, devem-se buscar formas alternativas que permitam verificar, segundo critérios de economia e de factibilidade, a validade de proposições efetuadas acerca do sistema formal em estudo. Dentre as técnicas mais largamente empregadas para tal finalidade destacam-se as demonstrações por indução matemática e as provas por contradição, estas também conhecidas por demonstrações por redução ao absurdo. Além destas, serão também apresentadas as técnicas de prova por contraposição (contrapositiva), por construção (prova direta), por análise de casos e por contraexemplos. Antes, porém, faremos uma apresentação das principais técnicas de provas usadas quando os respectivos enunciados envolvem apenas conjuntos.

Provas envolvendo conjuntos

Nestes casos, geralmente deve-se provar que dois conjuntos A e B quaisquer, construídos de forma diferentes, são iguais ou então que um é subconjunto do outro. Para a igualdade $(A = B)$, deve-se:

- Provar que todo elemento de A é também elemento de B (ou seja, $x \in A \Rightarrow x \in B$).

- Provar que todo elemento de B é também elemento de A (ou seja, $x \in B \Rightarrow x \in A$).

Para provar que um conjunto é subconjunto de outro ($A \subseteq B$), basta o primeiro item acima. Para provar que um conjunto é subconjunto próprio de outro ($A \subset B$), é necessário:

- Provar que todo elemento de A é também elemento de B.
- Provar que existe (pelo menos um) elemento de B que não é elemento de A.

Exemplo 1.54 Deseja-se provar que $(A \cap A) = A$, para qualquer conjunto A. Então:

- Suponha que $x \in A \cap A$. Logo, $x \in A$ e $x \in A$, ou seja, $x \in A$.
- Suponha que $x \in A$. Então $x \in A$ e $x \in A$ e, além disso, $x \in (A \cap A)$.

Em ambos os casos, a conclusão é verdadeira e isso encerra a prova. ⋆

Exemplo 1.55 Deseja-se provar que $(A \cap B) \subseteq B$, para quaisquer conjuntos A e B. Então:

- Considere $x \in A \cap B$. Logo, $x \in A$ e $x \in B$, ou seja, $x \in B$.
- Considere $x \in B$. Então $x \in A$ ou $x \notin A$. No primeiro caso, $x \in (A \cap B)$. No segundo, $x \notin (A \cap B)$.

Portanto, a relação de inclusão própria só é verificada se existir $x \in B$ tal que $x \notin A$. ⋆

Indução matemática

O princípio da **indução matemática** foi estabelecido com o intuito de permitir a generalização de uma propriedade P para um conjunto infinito de elementos X. Informalmente, indução é definida como uma "operação mental que consiste em se estabelecer uma verdade universal ou proposição geral com base no conhecimento de certo número de dados singulares ou de proposições de menor generalidade" (*Novo Dicionário Aurélio da Língua Portuguesa*).

Formalmente, o princípio da indução é estabelecido da seguinte forma:

- Inicialmente, elege-se um elemento ou subconjunto de elementos destacados de X, denominado **base da indução**, e demonstra-se que a propriedade P é válida neste caso particular. Geralmente, essa parte da prova é trivial.
- Admite-se, em seguida, que a propriedade seja válida para subconjuntos finitos de X que contenham o elemento utilizado para demonstrar a base da indução. Essa etapa é conhecida como **hipótese indutiva**, e é formulada, de maneira recorrente, nos próprios termos da propriedade que se deseja demonstrar.
- A seguir, confinado no fato de que, de maneira recorrente, a hipótese indutiva é verdadeira, demonstra-se que, se P é válida para um determinado elemento ou subconjunto de X, então P continuará sendo válida quando se acrescenta mais um elemento ao conjunto X (ou seja, P é válida para subconjuntos sucessivamente mais abrangentes de X). Essa etapa recebe a denominação de **passo indutivo**, e realiza a generalização da propriedade proposta.

Exemplo 1.56 Deseja-se provar que a propriedade $P_0(n) : 1 + 2^n < 3^n, \forall n \geqslant 2$ é válida para todos os números naturais maiores que 1.

- Base da indução:
  - $n = 2$;
  - $P_0(2) = 1 + 2^2 = 5 < 9$. Portanto, P_0 é válida para $n = 2$.
- Hipótese indutiva:

  - $P_0(k)$ é válida para $k \geqslant 2$, ou seja, $1+2^k < 3^k, k \geqslant 2$.

- Passo indutivo:
  - $P_0(k)$ implica $P_0(k+1), k \geqslant 2$;
  - Prova:
    * Pela hipótese indutiva: $P_0(k) = 1+2^k < 3^k, k \geqslant 2$;
    * Multiplicando-se ambos os membros da desigualdade por $2: 2+2^{k+1} < 2*3^k$;
    * Subtraindo-se 1 de ambos os membros da desigualdade: $1+2^{k+1} < 2*3^k - 1$;
    * Como $2x-1 < 3x, \forall x \geqslant 1$ (como $2x = 2x$ e, por hipótese, $x \geqslant 1$, segue que $2x-1 < 2x+x$, ou seja, $2x-1 < 3x$), então $1+2^{k+1} < 2*3^k - 1 < 3*3^k = 3^{k+1}$;
    * Portanto, $1+2^{k+1} < 3^{k+1} = P_0(k+1)$, ou seja, $P_0(n), \forall n \geqslant 2$.

A título de complementação deste exemplo, pode-se demonstrar, também por indução, que a propriedade $P_1(n): 2n-1 < 3n, \forall n \geqslant 1$, empregada na demonstração acima, é verificada no intervalo especificado. Na prática, a necessidade de se demonstrar passos ou hipóteses intermediárias em geral varia, conforme seja ou não intuitivo aceitar as afirmações apresentadas.

- Base da indução:
  - $n = 1$;
  - $P_1(1) = 2*1-1 = 1 < 3$.

- Hipótese indutiva:
  - $P_1(k)$ é válida para $k \geqslant 1$, ou seja, $2k-1 < 3k, \forall k \geqslant 1$.

- Passo indutivo:
  - $P_1(k)$ implica $P_1(k+1), k \geqslant 1$;
  - Prova:
    * Pela hipótese indutiva: $P_1(k) = 2k-1 < 3k, k \geqslant 1$;
    * Somando-se 2 a ambos os membros da desigualdade: $2k+1 < 3k+2$;
    * Como $3x < 3x+1, \forall x \geqslant 1$;
    * Então $2k+1 < 3k+2 < 3k+3$, ou seja, $2k+1 < 3k+3$;
    * Logo, $2(k+1)-1 < 3(k+1) = P_1(k+1)$, ou $P_1(n), \forall n \geqslant 1$.

$\star$

Exemplo 1.57 Demonstrar, por indução, que $P_2(n): \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

- Base da indução:
  - $n = 0$;
  - $P_2(0): \sum_{i=0}^{0} i = \frac{0(0+1)}{2} = 0$.

- Hipótese indutiva:
  - $P_2(k): \sum_{i=0}^{k} i = \frac{k(k+1)}{2}, k \geqslant 0$.

- Passo indutivo:

- $P_2(k)$ implica $P_2(k+1), k \geqslant 0$;
- Prova:
  - Pela hipótese indutiva, $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}, k \geqslant 0$;
  - Somando-se (k+1) a ambos os membros da igualdade: $\sum_{i=0}^{k} i + (k+1) = \sum_{i=0}^{k+1} i = \frac{k(k+1)}{2} + (k+1)$;
  - Desmembrando: $\frac{k(k+1)}{2} + (k+1) = \frac{k^2+k+2k+2}{2} = \frac{k^2+3k+2}{2}$;
  - Fatorando: $\frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2} = \frac{(k+1)((k+1)+1)}{2}$;
  - Logo, $\sum_{i=0}^{k+1} i = \frac{(k+1)((k+1)+1)}{2} = P_2(k+1)$.

⋆

Exemplo 1.58 Demonstrar, por indução, que $P_3(n) = \sum_{i=0}^{n} i^3 = \left(\sum_{i=0}^{n} i\right)^2, \forall n \geqslant 0$.

- Base da indução:
  - $n = 0$;
  - $\sum_{i=0}^{0} i^3 = \left(\sum_{i=0}^{0} i\right)^2 = 0$.
- Hipótese indutiva:
  - $\sum_{i=0}^{k} i^3 = \left(\sum_{i=0}^{k} i\right)^2, \forall k \geqslant 0$.
- Passo indutivo:
  - $P_3(k)$ implica $P_3(k+1), k \geqslant 0$;
  - Prova:
    - Pela hipótese indutiva, $\sum_{i=0}^{k} i^3 = \left(\sum_{i=0}^{k} i\right)^2, \forall k \geqslant 0$;
    - Somando-se $(k+1)^3$ a ambos os membros da igualdade, $\sum_{i=0}^{k} i^3 + (k+1)^3 = \left(\sum_{i=0}^{k} i\right)^2 + (k+1)^3 = \sum_{i=0}^{k+1} i^3$;
    - De acordo com o exemplo anterior, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}, \forall n \geqslant 0$;
    - Logo, $\left(\sum_{i=0}^{k} i\right)^2 + (k+1)^3 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$;
    - Desmembrando: $\left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)(k+1)^2$;
    - Fatorando: $\frac{k^2(k+1)^2}{4} + (k+1)(k+1)^2 = (k+1)^2\frac{k^2+4k+4}{4}$;

* Fatorando novamente:
  $(k+1)^2\frac{k^2+4k+4}{4} = (k+1)^2\left(\frac{k+2}{2}\right)^2 = \left((k+1)\left(\frac{k+2}{2}\right)\right)^2$;
* Como $\left((k+1)\left(\frac{k+2}{2}\right)\right)^2 = \left((k+1)\left(\frac{(k+1)+1}{2}\right)\right)^2 = \left(\sum_{i=0}^{k+1} i\right)^2$;
* Então $\sum_{i=0}^{k} i^3 + (k+1)^3 = \sum_{i=0}^{k+1} i^3 = \left(\sum_{i=0}^{k+1} i\right)^2 = P_3(k+1)$.

⋆

Os Exemplos 1.56, 1.57 e 1.58 demonstram a validade de proposições sobre subconjuntos dos números naturais. Na prática, no entanto, proposições sobre outros tipos de conjuntos, e não apenas $\mathbb{N}$, podem ser formuladas, mantendo-se a aplicabilidade integral dos princípios e das técnicas ilustradas nos exemplos.

Construção

Uma prova por **construção** (também conhecida como prova **direta** ou prova **dedutiva**) é uma prova em que a conclusão é obtida diretamente a partir das hipóteses, por meio de manipulações variadas. Nesses casos, a proposição geralmente se apresenta na forma de uma implicação "se H então C", com uma hipótese que deve ser assumida (H) e uma conclusão que se deseja provar (C). Usando o simbolo $\Rightarrow$ para representar a implicação lógica, podemos escrever $H \Rightarrow C$. Técnicas de reescrita (por exemplo, se $x = y$ e $y = z$, então pode-se inferir que $x = z$) e de simplificação (por exemplo, $x = y + 6/2$ torna-se $x = y + 3$) são bastante usadas neste método, assim como o enunciado de outros lemas e teoremas já provados.

Se $A \Rightarrow B$, diz-se que A é a **condição suficiente** (já que basta a validade de A para garantir a validade de B) e que B é a **condição necessária** (já que a validade de B é observada sempre que a validade de A for verificada). A prova de uma bi-implicação ($A \Leftrightarrow B$) corresponde à prova de duas implicações, $A \Rightarrow B$ e $B \Rightarrow A$. Neste caso, diz-se que a primeira prova corresponde à prova da **condição necessária** e que a segunda prova corresponde à prova da **condição suficiente**.

Na lógica clássica, é possível expressar a implicação por meio da disjunção e da negação: $((A \Rightarrow B) \equiv (B \vee \neg A))$.

Exemplo 1.59 Deseja-se provar que a soma de dois números pares é também um número par. A prova, neste caso, será por construção. O enunciado, aqui, pode ser expresso como $\forall m, n, (m \text{ é par }) \wedge (n \text{ é par }) \Rightarrow (m+n)$ é par .

- Hipótese (H): sejam m e n dois números pares.
- Definição de número par: então, $m = 2 * x$ e $n = 2 * y$, para algum x e y inteiros.
- Manipulação: logo, $m + n = 2 * x + 2 * y = 2 * (x + y)$.
- Conclusão (C): ou seja, $m + n$ é também um número par, pois é múltiplo de 2.

⋆

Contraposição

Eventualmente é mais fácil provar uma proposição por meio da sua **contrapositiva**. A contrapositiva (na lógica clássica) de uma proposição do tipo "se H então C" ($H \Rightarrow C$) corresponde à proposição "se não C então não H" ($\overline{C} \Rightarrow \overline{H}$). Como se pode verificar, as tabelas-verdade

das duas proposições são idênticas. Portanto, a prova de que a contrapositiva é verdadeira pode ser usada como prova de que a proposição original também é verdadeira.

Exemplo 1.60 Deseja-se provar que, se a soma de dois números é par, então os dois são pares ou os dois são impares. Em outras palavras, $(m+n)$ é par $\Rightarrow (m$ é par $\wedge n$ é par $) \vee (m$ é ímpar $\wedge n$ é impar $)$. A contrapositiva, neste caso, pode ser representada como:

$$\overline{(m \text{ é par } \wedge n \text{ é par }) \vee (m \text{ é ímpar } \wedge n \text{ é ímpar })} \Rightarrow \overline{(m+n) \text{ é par}}$$

ou ainda:

$$\overline{m \text{ é par } \wedge n \text{ é par}} \wedge \overline{m \text{ é ímpar } \wedge n \text{ é ímpar}} \Rightarrow \overline{(m+n) \text{ é par}}$$

ou ainda:

$$(m \text{ é ímpar } \vee n \text{ é ímpar }) \wedge (m \text{ é par } \vee n \text{ é par }) \Rightarrow \overline{(m+n) \text{ é par}}$$

ou ainda:

$$(m \text{ é ímpar } \vee n \text{ é ímpar }) \wedge (m \text{ é par } \vee n \text{ é par }) \Rightarrow (m+n) \text{ é ímpar}$$

Como um número não pode ser simultaneamente par e ímpar, segue que existem apenas duas possibilidades para a hipótese ser verdadeira:

- m é ímpar e n e par, ou
- m é par e n e ímpar.

No primeiro caso, temos que $m = 2*x+1$ e $n = 2*y$. Logo, $m+n = 2*x+1+2*y = 2*(x+y)+1$, portanto ímpar. No segundo caso, temos que $m = 2*x$ e $n = 2*y+1$. Logo, $m+n = 2*x+2*y+1 = 2*(x+y)+1$, portanto ímpar também. ⋆

Exemplo 1.61 Repetiremos, agora, a demonstração do teorema do Exemplo 1.59, usando a técnica contrapositiva. Deseja-se provar, por contraposição, que a soma de dois números pares é também um número par. A contrapositiva, neste caso, é a proposição "se um número não é par, então ele não pode ser a soma de dois números pares". Essa contrapositiva pode ser expressa como $\overline{(m+n)}$ é par $\Rightarrow$ $\overline{m \text{ é par } \wedge n \text{ é par}}$, ou ainda $(m+n)$ é ímpar $\Rightarrow m$ é ímpar $\vee n$ é ímpar .

- Hipótese (H): $m+n$ é ímpar.
- Definição de número ímpar: então, $m+n = 2*x+1$, para algum x inteiro.
- Definição de número par: logo, $2*x$ é um número par.
- Teorema anterior: conforme o Exemplo 1.60, $2*x$ deve ser a soma de dois números pares ou de dois números ímpares. Suponha que estes números sejam p e q e, portanto, $2*x = p+q$.
- Consequência: ($p = 2*z+1$ e $q = 2*w+1$) ou ($p = 2*z$ e $q = 2*w$).
- Manipulação: $m+n = 2*x+1 = p+q+1$.
- Conclusão: no primeiro caso, temos que $m+n = 2*z+1+2*w+1 = 2*(z+w+1)$ que é par; no segundo caso, temos que $m+n = 2*z+2*w = 2*(z+w)$ que é par também, e isso conclui a prova.

⋆

Contradição

Uma outra técnica bastante popular utilizada na demonstração de teoremas (na lógica clássica) é a demonstração por contradição.

A essência da técnica da demonstração por **contradição** (ou **redução ao absurdo**) consiste em adotar como base da demonstração a negação da hipótese formulada e, através de manipulações lógicas, mostrar que a negação dessa hipótese conduz a um paradoxo, muitas vezes correspondente à sua própria contradição. Dessa forma, a hipótese negada não pode ser considerada verdadeira, devendo, portanto, ser considerada falsa, e, consequentemente, a hipótese original deve ser considerada verdadeira.

Exemplo 1.62 Deseja-se provar, por redução ao absurdo, que $\sqrt{2}$ não pode ser expressa como um número racional, ou seja, como fração cujo numerador e denominador, respectivamente p e q, são números inteiros (conforme [4]). Admitindo-se a hipótese como verdadeira (negação da hipótese original), então:

$$\sqrt{2} = \frac{p}{q}$$

Pode-se considerar, sem perda de generalidade, que p e q não possuem fatores comuns. Caso haja fatores comuns, simplifica-se a fração antes de iniciar o procedimento. Elevando-se ambos os lados da igualdade ao quadrado, obtém-se:

$$2 = \frac{p^2}{q^2}, \text{ ou } p^2 = 2q^2$$

Portanto, p^2 e, consequentemente, p são números pares. Substituindo-se p por $2m$ na equação acima, temos:

$(2m)^2 = 2q^2$, ou $q^2 = 2m^2$

Isso mostra que q^2 e, portanto, q também são números pares. Ora, se p e q são pares, isso contradiz a hipótese original de que entre eles não haveria fatores comuns. Dessa forma, a hipótese não pode ser verdadeira, concluindo-se que a raiz quadrada de 2 não pode ser um número racional. ⋆

Análise de casos

Uma prova por **análise de casos** é uma prova que é dividida em um número finito de casos, os quais devem todos ser provados individualmente a fim de garantir a validade da proposição original. Trata-se, pois, de garantir que a proposição é verdadeira em qualquer cenário considerado, os quais envolvem, normalmente, todos os possíveis valores para as suas variáveis.

Exemplo 1.63 Conside a contrapositiva do Exemplo 1.61, $(m+n)$ é ímpar $\Rightarrow m$ é ímpar $\vee n$ é ímpar . Só existem quatro casos para serem analisados:

- m é par e n é par;
  Neste caso, $m+n$ é par;
- m é par e n é ímpar;
  Aqui, $m+n$ é ímpar;
- m é ímpar e n é par;
  Também aqui, $m+n$ é ímpar;
- m é ímpar e n é ímpar;
  Neste caso, $m+n$ é par.

Logo, os únicos casos em que $(m+n)$ é ímpar são (i) quando m é par e n é ímpar, ou (ii) quando m é ímpar e n é par, e isso conclui a prova. ⋆

Exemplo 1.64 Deseja-se provar a comutatividade da conjunção: $\forall p, \forall q, p \wedge q = q \wedge p$. Numa análise de casos, consideram-se todos os possíveis valores para as variáveis p e q ("F" para Falso e "V" para Verdadeiro), como no Exemplo 1.51. ⋆

Exemplos e contraexemplos

Quando o enunciado da proposição envolve a prova da existência de um objeto, uma técnica de prova que pode ser usada é justamente demonstrar a existência de um objeto com as propriedades exigidas (para atestar a validade da proposição). Caso a proposição estabeleça a inexistência de tal objeto, a prova da sua existência serve para demonstrar a falsidade da proposição.

Exemplo 1.65 Sejam $A = \{1,2,3\}$ e $B = \{3,4,5\}$. Deseja-se provar que existe um elemento que pertence aos dois conjuntos simultaneamente. A prova, neste caso, envolve a menção ao elemento 3. De fato, $3 \in A$ e $3 \in B$, e isso valida a proposição. ⋆

Exemplo 1.66 Sejam $A = \{1,2,3\}$ e $B = \{3,4,5\}$. Deseja-se provar que não existe um elemento que pertence aos dois conjuntos simultaneamente. A prova, neste caso, envolve também a menção ao elemento 3. De fato, $3 \in A$ e $3 \in B$, e isso invalida a proposição. ⋆

1.8 Conjuntos enumeráveis

Quando se estudam os conjuntos, frequentemente torna-se necessário compará-los entre si em relação à quantidade de elementos neles contidos, ou seja, à sua **cardinalidade**.

A cardinalidade de um conjunto é uma medida da quantidade de elementos contidos nele, ou seja, da grandeza que intuitivamente é conhecida como "tamanho" do conjunto.

Trata-se de um conceito de fácil compreensão quando referente a conjuntos finitos. Nesse caso, diz-se que dois conjuntos A e B têm a mesma cardinalidade se eles possuírem a mesma quantidade de elementos, ou seja, $|A| = |B|$. Se A possuir mais elementos que B, escreve-se $|A| > |B|$.

A cardinalidade de um conjunto finito é, portanto, simplesmente o número natural que informa a quantidade de elementos que compõem esse conjunto. Quando se trata de conjuntos finitos, tais resultados são intuitivos e, até certo ponto, óbvios. Por exemplo, se X for um subconjunto próprio de Y, então ter-se-á sempre $|X| < |Y|$.

Exemplo 1.67 Considerem-se os conjuntos finitos $A = \{a,b,c,d\}$ e $B = \{0,1,2,3,4,5\}$. Então, $|A| = 4, |B| = 6$ e $|A| < |B|$. ⋆

De que forma seria, por outro lado, possível comparar o "tamanho" de dois conjuntos infinitos? Assim como no caso dos conjuntos finitos, dois conjuntos infinitos também podem possuir a mesma cardinalidade, bastando para isso que seja possível identificar uma correspondência biunívoca entre os elementos de ambos os conjuntos.

Formalmente, diz-se que dois conjuntos A e B quaisquer, finitos ou infinitos, possuem a mesma cardinalidade, ou seja, $|A| = |B|$, se for possível definir entre eles uma função bijetora.

Exemplo 1.68 Sejam $A = \{a,b,c\}$ e $B = \{7,3,6\}$. Neste exemplo, A e B possuem a mesma cardinalidade, pois $|A| = |B| = 3$. Note-se que é possível definir uma função bijetora de A para B: $\{(a,7), (b,3), (c,6)\}$. Naturalmente, muitas outras funções bijetoras também podem ser definidas entre esses dois conjuntos. ⋆

Exemplo 1.69 Sejam $A = \{a \mid a \text{ é ímpar}, 1 \leqslant a \leqslant 100\}$ e $B = \{b \mid b \text{ é par}, 1 \leqslant b \leqslant 100\}$. A e B são conjuntos finitos que possuem a mesma cardinalidade, pois a função $f(a) = a + 1$ é bijetora, mapeando os elementos do conjunto A nos elementos do conjunto B. Neste caso, $|A| = |B| = 50$. ⋆

Exemplo 1.70 Considere-se o conjunto dos números inteiros $\mathbb{Z}$ e o subconjunto de $\mathbb{Z}$ composto apenas pelos números ímpares. Trata-se, naturalmente, de dois conjuntos infinitos, sendo o segundo um subconjunto próprio do primeiro. Porém, de acordo com a definição, embora isso pareça paradoxal, os dois conjuntos possuem a mesma cardinalidade, já que a função bijetora $2 * i + 1$, onde $i \in \mathbb{Z}$, mapeia univocamente cada elemento de $\mathbb{Z}$ em um único elemento do conjunto dos números ímpares. ⋆

Do Exemplo 1.70 pode-se observar facilmente que, diferentemente do que ocorre com conjuntos finitos, é possível, para conjuntos infinitos, definir subconjuntos próprios com a mesma cardinalidade do conjunto original.

Caso não seja possível identificar pelo menos uma função bijetora entre dois conjuntos A e B quaisquer, é ainda possível que se constate a existência de uma função total e injetora de A para B. Neste caso, diz-se que $|A| \leqslant |B|$. Se, além disso, for possível provar a inexistência de uma função bijetora de A para B, então $|A| < |B|$.

Diz-se que um conjunto é **enumerável**, ou simplesmente **contável**, se ele possuir um número finito de elementos, ou então, no caso de ser infinito, se ele possuir a mesma cardinalidade que o conjunto dos números naturais $\mathbb{N}$. Conjuntos infinitos X tais que $|X| \neq |\mathbb{N}|$ são ditos **não enumeráveis** ou **não contáveis**.

O conceito de conjuntos enumeráveis está diretamente relacionado ao conceito intuitivo de "sequencialização" dos elementos de um conjunto, com o objetivo de permitir a sua contagem. Na prática, a operação de contagem de elementos de um conjunto pode ser definida como o estabelecimento de uma correspondência única (função bijetora) entre o conjunto dos números naturais e o conjunto cujos elementos se pretenda contar.

A sequencialização é uma operação que visa estabelecer uma relação de ordem entre os elementos de um conjunto (efetuar a sua ordenação) para permitir a associação unívoca de cada um de seus elementos com os correspondentes elementos de $\mathbb{N}$.

Exemplo 1.71 O conjunto dos números inteiros $\mathbb{Z}$ é um exemplo de conjunto infinito enumerável. A ordenação apresentada na Tabela 1.8 ilustra uma sequencialização que permite associar os elementos de $\mathbb{Z}$ com os de $\mathbb{N}$. Essa associação também pode ser representada por meio da função:

$$f(n) = (-1)^{n+1} * \frac{n + (n \bmod 2)}{2}$$

⋆

Tabela 1.8 Bijeção entre $\mathbb{N}$ e $\mathbb{Z}$

$\mathbb{Z}$	0	1	-1	2	-2	3	-3	...
$\mathbb{N}$	0	1	2	3	4	5	6	...

Exemplo 1.72 O conjunto formado pelos pares ordenados $(x,y) \in \mathbb{N} \times \mathbb{N}$, com $x > y$, também constitui um exemplo de conjunto infinito enumerável. Isso pode ser percebido com o auxílio da Tabela 1.9, em que um arranjo bidimensional permite visualizar a sequencialização desses pares, de modo que seja possível estabelecer a sua associação com os elementos de $\mathbb{N}$.

A associação com $\mathbb{N}$ pode ser feita imaginando-se uma linha que percorra todos os elementos dessa matriz a partir do canto superior esquerdo, conforme a sequência geométrica mostrada na Tabela 1.9. Desse modo, a seguinte sequência de pares é obtida:

$$(1,0),(2,0),(3,0),(2,1),(3,1),(4,0),(5,0),(4,1),(3,2)...$$

Tal sequência pode ser facilmente colocada em correspondência com os elementos de $\mathbb{N}$, conforme ilustrado na Tabela 1.10. Técnica semelhante pode ser usada para demonstrar que o conjunto $\mathbb{N} \times \mathbb{N}$ e o conjunto $\mathbb{Q}$ dos números racionais também são enumeráveis. Neste último caso, em particular, basta considerar o elemento $(x,y) \in \mathbb{N} \times \mathbb{N}$ como uma representação da fração x/y (a fim de evitar o denominador zero, a primeira coluna do arranjo deve ser omitida). ⋆

Exemplo 1.73 O conjunto $\mathbb{R}$, composto pelos números reais, constitui um exemplo de conjunto infinito não enumerável, uma vez que, como demonstrado a seguir, $|\mathbb{R}| \neq |\mathbb{N}|$. Para efetuar essa demonstração, será considerado o seguinte subconjunto de $\mathbb{R}$:

$$S = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

O gráfico da Figura 1.15 ilustra o comportamento da função $f(x)$ no intervalo 0 a 1. Como se pode perceber, ela efetua um espalhamento do seu domínio de forma a mapear os elementos dele em elementos de $\mathbb{R}$.

Tabela 1.9 $\{(x,y) \in \mathbb{N} \times \mathbb{N} \mid x > y\}$ é um conjunto enumerável

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	...
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	...
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	...
(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	...
(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	...
(5,0)	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	...
⋮	⋮	⋮	⋮	⋮	⋮	

Tabela 1.10 Bijeção entre $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$

$\mathbb{Z} \times \mathbb{Z}$	(1,0)	(2,0)	(3,0)	(2,1)	...
$\mathbb{N}$	0	1	2	3	...

A prova de que $\mathbb{R}$ é não enumerável é efetuada em dois passos: inicialmente demonstra-se que S possui a mesma cardinalidade que $\mathbb{R}$, e a seguir demonstra-se que S é um conjunto não enumerável. O fato de que $|S| = |\mathbb{R}|$ pode ser constatado pela existência da função bijetora f, apresentada a seguir, a qual permite associar univocamente elementos de S com elementos de $\mathbb{R}$:

$$f(x) = \begin{cases} \dfrac{1}{2x} - 1, & 0 < x < 0,5 \\ \dfrac{1}{2(x-1)} + 1, & 0,5 \leqslant x < 1 \end{cases}$$

A prova de que S é um conjunto não enumerável é feita por contradição, ou seja, mostrando-se que, qualquer que seja a sequencialização proposta para os elementos de S, sempre será possível identificar um novo elemento de S que não pertence à sequência apresentada. Desse modo, a hipótese original de que S é um conjunto enumerável deve ser considerada inválida.

Admita-se que exista uma sequencialização de S de tal modo que seja possível associar cada elemento desse conjunto univocamente a elementos de $\mathbb{N}$. Assim, seria obtida uma associação do tipo ilustrado pela Tabela 1.11.

Suponha-se, sem perda de generalidade, que todos os elementos de S sejam denotados através de representações com um número infinito de casas de decimais significativas. Assim, por exemplo, em vez de escrever $0,1$, adota-se a representação equivalente:

$$0,099999999999999999999999...$$

Se cada elemento $\mathbb{R}_i \in S$ pode ser escrito como sendo uma sequência infinita do tipo:

$$0, d_{i_0} d_{i_1} d_{i_2} d_{i_3} ... d_{i_n} ...$$

então a construção do novo elemento:

$$0, x_0 x_1 x_2 x_3 ... x_n ..., x_j \neq d_{j_j}, x_j \neq 0$$

é suficiente para provar que ele não pertence à sequência originalmente proposta, uma vez que esse novo elemento difere em pelo menos uma casa decimal de cada um dos elementos inicialmente considerados, sendo, portanto, diferente de todos eles. Sejam:

$$\mathbb{R}_0 \quad = \quad 0, \underbrace{d_{0_0}} \, d_{0_1} d_{0_2} d_{0_3} ... d_{0_n} ...$$

$$\begin{aligned}
\mathbb{R}_1 &= 0, d_{1_0} \underbrace{d_{1_1}} d_{1_2} d_{1_3} ... d_{1_n} ... \\
\mathbb{R}_2 &= 0, d_{2_0} d_{2_1} \underbrace{d_{2_2}} d_{2_3} ... d_{2_n} ... \\
\mathbb{R}_3 &= 0, d_{3_0} d_{3_1} d_{3_2} \underbrace{d_{3_3}} ... d_{3_n} ... \\
... &= ...
\end{aligned}$$

Então, escolhe-se $0, x_0 x_1 x_2 x_3 ... x_n ...$ com $x_0 \neq d_{0_0}$, $x_1 \neq d_{1_1}$, $x_2 \neq d_{2_2}$, $x_3 \neq d_{3_3}$ etc. Logo, S não é enumerável e, consequentemente, $\mathbb{R}$ também não. ⋆

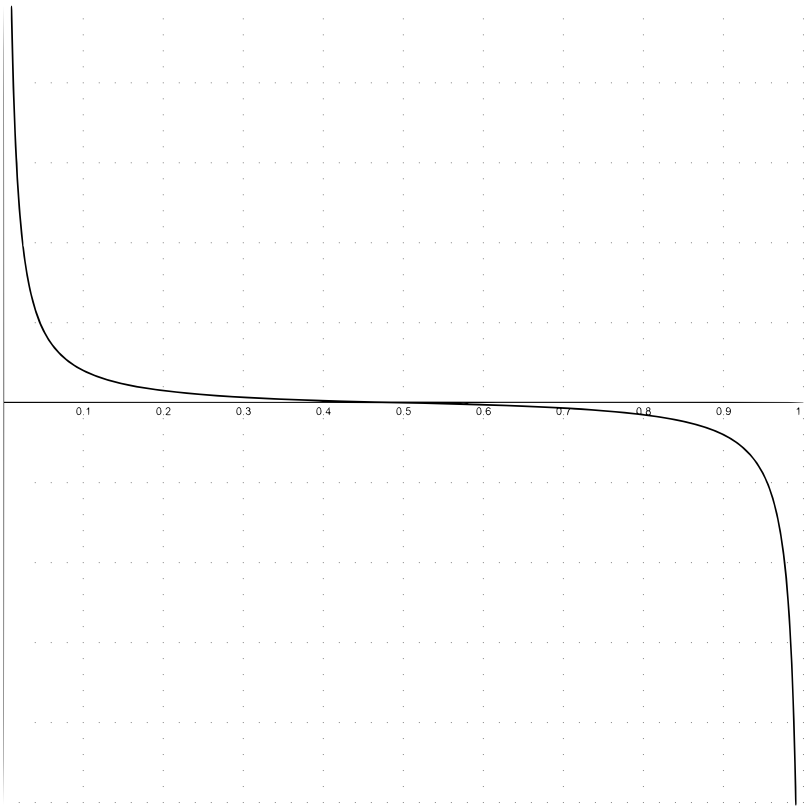


Figura 1.15 Comportamento de $f(x)$.

Tabela 1.11 Bijeção hipotética entre $\mathbb{N}$ e S

S	$\mathbb{R}_0$	$\mathbb{R}_1$	$\mathbb{R}_2$	$\mathbb{R}_3$	...
$\mathbb{N}$	0	1	2	3	...

Como está mostrado no Exemplo 1.73, nem todos os conjuntos infinitos possuem a mesma cardinalidade. Assim, apesar de $\mathbb{N}$ e $\mathbb{R}$ possuírem uma quantidade infinita de elementos, é intuitivo que $\mathbb{R}$ possui uma quantidade muito maior de elementos que $\mathbb{N}$, ou seja, $|\mathbb{R}| > |\mathbb{N}|$, impedindo que seja estabelecida uma função bijetora entre ambos.

Esses são alguns dos resultados da Teoria dos Números Transfinitos ([5]), desenvolvida no final do século XIX pelo matemático russo Georg Cantor (1845-1918), de acordo com a qual os **números transfinitos** representam quantidades não finitas ordenadas de forma crescente. Tais quantidades são representadas por $\aleph_0, \aleph_1, ..., \aleph_n, ...$,[2] de tal forma que $\aleph_{i-1} < \aleph_i < \aleph_{i+1}$, para $i \geqslant 1$. Além disso, $\aleph_0 = |\mathbb{N}|$.

Outros exemplos de conjuntos infinitos enumeráveis são o conjunto dos números racionais e o conjunto de todas as cadeias que podem ser formadas pela concatenação de símbolos de um conjunto finito Σ. Já o conjunto formado por todos os subconjuntos de $\mathbb{N}$, ou seja, o conjunto $2^{\mathbb{N}}$, é não enumerável.

Formalmente, um conjunto X é dito **infinito** se for possível identificar um subconjunto próprio de X, por exemplo, Y, tal que $|X| = |Y|$.

Exemplo 1.74 No Exemplo 1.73, o fato de que $S \subset \mathbb{R}$ e $|S| = |\mathbb{R}|$ é suficiente para garantir que $\mathbb{R}$ é um conjunto infinito. ⋆

Exemplo 1.75 Considere-se o conjunto dos números naturais $\mathbb{N}$. Deseja-se demonstrar que $\mathbb{N}$ é infinito com o auxílio do subconjunto próprio $\mathbb{N} - \{0\}$. Não é difícil perceber que esses dois conjuntos possuem a mesma cardinalidade, uma vez que a função $n+1, n \in \mathbb{N}$ mapeia univocamente cada elemento de $\mathbb{N}$ em elementos do subconjunto próprio $\mathbb{N} - \{0\} : 0 \to 1, 1 \to 2, 2 \to 3, 3 \to 4, 4 \to 5, 5 \to 6, 6 \to 7...$

Assim, apesar de $\mathbb{N} - \{0\}$ possuir um elemento a menos que $\mathbb{N}$, na verdade ambos possuem a mesma cardinalidade, o que confirma $\mathbb{N}$ como conjunto infinito. ⋆

A seguir serão apresentados e demonstrados alguns dos principais resultados teóricos sobre conjuntos enumeráveis e não enumeráveis. Antes do primeiro teorema, no entanto, será apresentado o Método Diagonal de Cantor.

Método Diagonal de Cantor

O Método Diagonal de Cantor foi publicado por Georg Cantor em 1891 e é bastante utilizado até os dias de hoje. Ele mostra como obter um conjunto diferente de todos os conjuntos de uma dada coleção de conjuntos, seja ela finita ou infinita. Cada um dos conjuntos dessa coleção, por sua vez, pode conter um número finito ou infinito de elementos. O número de elementos usados para caracterizar tais conjuntos também pode ser finito ou infinito.

Entre algumas aplicações do Método, pode-se citar a prova de que $|2^A| > |A|$, para qualquer conjunto A, (Teorema 1.5) e a prova de que a linguagem L_D não é recursivamente enumerável (Teorema 7.16).

O uso do Método é ilustrado por meio de uma matriz com linhas e colunas. Cada coluna representa um certo elemento (podem existir infinitas colunas). Cada linha representa um conjunto criado com esses elementos (se a quantidade de colunas for infinita, podem existir infinitos conjuntos). O cruzamento de uma linha com uma coluna é marcado para indicar se aquele elemento pertence (1) ou não pertence (0) ao respectivo conjunto.

O Método utiliza a diagonal principal dessa matriz, denominada "vetor característico", e, em seguida, a sua complementação (0s se tornam 1s e vice-versa). Essa diagonal complementada é então considerada como um conjunto de elementos e, conforme se pode perceber, tal conjunto é diferente de todos os demais conjuntos presentes nas linhas da matriz, uma vez que difere de cada um deles por pelo menos um elemento. O novo conjunto assim construído é então usado para fazer a prova em questão.

[2] $\aleph$ (aleph) é a primeira letra do alfabeto hebraico.

Exemplo 1.76 Suponha que os elementos são números naturais (cada coluna representa, portanto, um número natural). Cada linha representa um subconjunto dos números naturais. Quaisquer que sejam os conjuntos considerados nas linhas, a complementação da diagonal principal produz um novo subconjunto desses mesmos elementos que difere de todos os considerados nas linhas da matriz (Tabela 1.12).

Tabela 1.12 Método Diagonal de Cantor

	0	1	2	3	4	...
S_0	1	1	1	0	1	...
S_1	1	1	0	0	1	...
S_2	1	0	0	1	0	...
S_3	0	1	1	1	0	...
S_4	0	0	1	0	0	...
...	...	...	...	...	...	...

Na Tabela 1.12, prenchida com 0s e 1s de forma aleatória, temos:

- $S_0 = \{0,1,2,4,...\}$.
- $S_1 = \{0,1,4,...\}$.
- $S_2 = \{0,3,...\}$.
- $S_3 = \{1,2,3,...\}$.
- $S_4 = \{2,...\}$.
- Diagonal principal: 11010....
- Diagonal principal complementada: 00101....
- Conjunto obtido pela diagonal principal complementada: $X = \{2,4,...\}$.
- $X \neq S_i, i \geqslant 0$.

Ou seja, o conjunto X, obtido pela complementação da diagonal principal, é diferente de todos os conjuntos S_i, em todas as linhas. ⋆

Teorema 1.5 (Teorema de Cantor) "Seja A um conjunto qualquer. Então $|2^A| > |A|$."

Constata-se com facilidade a existência de pelo menos uma função f, que associa cada elemento $x \in A$ com um elemento $f(x) \in 2^A$, e que seja injetora e total (no caso, $f(x) = \{x\}$). Logo, é possível concluir que $|A| \leqslant |2^A|$. Para provar que $|A| < |2^A|$, é suficiente mostrar que não existe função bijetora entre A e 2^A. Suponha-se que exista tal bijeção, como ilustrado a seguir, onde S_i representa algum subconjunto de A:

Tabela 1.13 Função f para o Teorema 1.5

$A:$	x_0	x_1	x_2	x_3	x_4	$\cdots$
$f:$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
$2^A:$	S_0	S_1	S_2	S_3	S_4	$\cdots$

Nesse caso, pode-se afirmar que todo e qualquer elemento $x \in A$ está associado a um elemento distinto $f(x) \in 2^A$. Considere-se agora o seguinte subconjunto de A (obtido pela complementação da diagonal principal, conforme o Método Diagonal de Cantor):

$$S = \{x \in A \mid x \notin f(x)\}$$

O conjunto S é formado por todos os x_i que não são elementos do conjunto $f(x_i) = S_i$ correspondente (ou seja, todos os elementos $x_i \in A$ tais que os elementos e_{ii} da matriz, obtidos pelo cruzamento da coluna i com a coluna i, estejam preenchidos com 0).

De acordo com a hipótese formulada (de que existe uma bijeção entre os conjuntos), é esperado que $S = f(x_i)$ para algum $x_i \in A$. Tal conclusão, se verdadeira, acarretaria as seguintes consequências, de forma exclusiva:

- Se $x_i \in S$, e como $S = f(x_i)$, por hipótese, então $x_i \notin S$, o que constitui uma contradição.
- Se $x_i \notin S$, e como $S = \{x \in A \mid x \notin f(x)\}$, por definição, então $x_i \in S$, o que também é uma contradição.

Qualquer que seja o caso, resulta uma contradição. Logo, a hipótese inicialmente formulada é falsa e disso conclui-se não existir qualquer bijeção entre A e 2^A. Portanto, $|A| < |2^A|$.

Outra forma de concluir a prova consiste em perceber que o conjunto S é diferente de todos os conjuntos S_i da matriz (dos quais difere em pelo menos um elemento em cada). Logo, não existe a suposta bijeção entre A e 2^A. □

O Teorema 1.5 demonstra que conjuntos infinitos de cardinalidades sucessivamente maiores podem ser obtidos pela aplicação sucessiva da operação conjunto-potência. Considere os conjuntos $A, B = 2^A, C = 2^B, D = 2^C$ etc. Então, $|A| < |B| < |C| < |D| < ...$

Exemplo 1.77 O Teorema 1.5 pode ser usado para provar que $|\mathbb{N}| < |2^{\mathbb{N}}|$. É fácil notar que existe uma função injetora e total entre $\mathbb{N}$ e $2^{\mathbb{N}}$ (por exemplo, $f(0) = \{0\}, f(1) = \{1\}$ etc). Suponha agora que existe uma bijeção entre $\mathbb{N}$ e $2^{\mathbb{N}}$ (Tabela 1.14):

Tabela 1.14 Função f para o Exemplo 1.77

$\mathbb{N}$:	0	1	2	3	4	$\cdots$
f :	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	
$2^{\mathbb{N}}$:	S_0	S_1	S_2	S_3	S_4	$\cdots$

Considere o conjunto $S = \{x \in \mathbb{N} \mid x \notin f(x)\}$ (o conjunto S corresponde ao complemento da diagonal principal conforme o Método Diagonal de Cantor). Neste caso, temos que $S \neq S_i, \forall i \geq 0$, e, portanto, não pode existir bijeção entre $\mathbb{N}$ e $2^{\mathbb{N}}$. ⋆

De acordo com a teoria de Cantor, $\mathbb{N}$ é o conjunto que possui a menor cardinalidade entre todos os conjuntos infinitos, a qual é denotada por $\aleph_0$, o primeiro número da sua série transfinita. Conforme o Exemplo 1.77, $|\mathbb{N}| < |2^{\mathbb{N}}|$. Por outro lado, conforme foi visto anteriormente, $|\mathbb{N}| < |\mathbb{R}|$, o que sugere a questão: "será que $|\mathbb{R}| = |2^{\mathbb{N}}|$?". De fato, esse resultado pode ser provado como sendo verdadeiro (ver [6]).

Por outro lado, não se sabe da existência de algum conjunto X tal que $\aleph_0 < |X| < |\mathbb{R}|$ (ou, o que é equivalente, $\aleph_0 < |X| < |2^{\mathbb{N}}|$). Ou seja, não se sabe se existe algum conjunto infinito com cardinalidade estritamente maior que a do conjunto dos números naturais e estritamente menor que o conjunto dos números reais. A **Hipótese do Contínuo** (ver [6]) considera que não existe tal conjunto e, portanto, que $|\mathbb{R}| = \aleph_1$ (logo $|2^{\mathbb{N}}| = \aleph_1$).

Teorema 1.6 ($|B|, B \subseteq A, |A| = \aleph_0$) "Sejam A e B dois conjuntos, $B \subseteq A$. Se $|A| = \aleph_0$, então $|B| \leqslant \aleph_0$."

Se $|A| = \aleph_0$, então existe uma função bijetora entre o conjunto dos números naturais $\mathbb{N}$ e o conjunto A (e vice-versa). Logo, existe uma função injetora e total f_1 que associa elementos

Tabela 1.15 Função f_1 para o Teorema 1.6

A:	a_0	a_1	a_2	$\cdots$	a_n	$\cdots$
f_1 :	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	
$\mathbb{N}$:	0	1	2	$\cdots$	n	$\cdots$

de A e $\mathbb{N}$, conforme a Tabela 1.15. Se B é subconjunto de A, é possível associar cada elemento de B ao mesmo elemento de A através de uma função injetora e total f_2, conforme a Tabela 1.16. A composição das funções f_1 e f_2, ilustrada na Tabela 1.17, mostra que

Tabela 1.16 Função f_2 para o Teorema 1.6

B:	–	a_1	–	$\cdots$	a_n	$\cdots$
f_2 :		$\downarrow$			$\downarrow$	
A:	a_0	a_1	a_2	$\cdots$	a_n	$\cdots$

existe uma função injetora e total de B para $\mathbb{N}$. Logo, $|B| \leqslant |\mathbb{N}|$, ou seja, $|B| \leqslant \aleph_0$. Em outras

Tabela 1.17 Composição de f_1 com f_2 para o Teorema 1.6

B:	–	a_1	–	...	a_n	...
f_2 :		$\downarrow$			$\downarrow$	
A:	a_0	a_1	a_2	...	a_n	...
f_1 :	$\downarrow$	$\downarrow$	$\downarrow$		$\downarrow$	
$\mathbb{N}$:	0	1	2	...	n	...

palavras, qualquer subconjunto (finito ou infinito) de um conjunto enumerável é também um conjunto enumerável. □

Exemplo 1.78 Sabe-se que $\mathbb{Z}_+ \subseteq \mathbb{Z}$. Como $|\mathbb{Z}| = \aleph_0$, segue que $|\mathbb{Z}_+| = \aleph_0$. Por outro lado, $\{0,1,2,3\} \subseteq \mathbb{Z}$. Como $|\{0,1,2,3\}| = 4$, segue que $4 < \aleph_0$. ⋆

Teorema 1.7 ($|A \cup B|, |A| = \aleph_0, |B| = \aleph_0$) "Sejam A e B dois conjuntos quaisquer. Se $|A| = \aleph_0$ e $|B| = \aleph_0$, então $|A \cup B| = \aleph_0$."

Se A e B são conjuntos enumeráveis (finitos ou infinitos), então seus elementos podem ser ordenados da seguinte forma:

$$\begin{aligned} A: &\quad a_0, a_1, a_2, a_3, a_4, ...a_{n-1}, a_n, a_{n+1}... \\ B: &\quad b_0, b_1, b_2, b_3, b_4, ...b_{n-1}, b_n, b_{n+1}... \end{aligned}$$

A enumeração dos elementos de $A \cup B$ pode ser feita através do seguinte procedimento:

$$A \cup B : a_0, b_0, a_1, b_1, a_2, b_2, ...a_{n-1}, b_{n-1}, a_n, b_n, a_{n+1}, b_{n+1}, ...$$

Portanto, $A \cup B$ é enumerável e $|A \cup B| = \aleph_0$. Em outras palavras, a união de dois conjuntos enumeráveis é sempre um conjunto enumerável. □

Exemplo 1.79 Como $|\mathbb{Z}_+| = \aleph_0$ e $|\mathbb{Z}_-| = \aleph_0$, segue que $\mathbb{Z} = \mathbb{Z}_- \cup \mathbb{Z}_+$ e, portanto, $|\mathbb{Z}| = \aleph_0$. ⋆

Teorema 1.8 ($|A \cap B|, |A| = \aleph_0, |B| = \aleph_0$) "Sejam A e B dois conjuntos quaisquer. Se $|A| = \aleph_0$ e $|B| = \aleph_0$, então $|A \cap B| \leq \aleph_0$."

Se $A \subseteq B$, então $A \cap B = A$ e $|A \cap B| = |A| = \aleph_0$ por hipótese. Se, por outro lado, $B \subseteq A$, então $A \cap B = B$ e $|A \cap B| = |B| = \aleph_0$ por hipótese. Finalmente, se nenhuma dessas duas condições for verdadeira, então $(A \cap B) \subseteq A$ e, pelo Teorema 1.6, $|A \cap B| \leq \aleph_0$. Portanto, em qualquer caso que se considere, $|A \cap B| \leq \aleph_0$. □

Exemplo 1.80 Como $|\mathbb{Z}_+| = \aleph_0$ e $|\mathbb{Z}_-| = \aleph_0$, segue que $\mathbb{Z}_- \cap \mathbb{Z}_+ = \emptyset$, com $|\emptyset| = 0$ e, portanto, $0 < \aleph_0$. Por outro lado, seja $I = \{x \in \mathbb{Z} \mid x \text{ é ímpar}\}$. Como $|\mathbb{N}| = \aleph_0$ e $|I| = \aleph_0$, temos que $\mathbb{N} \cap I = \{x \in \mathbb{N} \mid x \text{ é ímpar}\}$ e $|\mathbb{N} \cap I| = \aleph_0$. ⋆

Teorema 1.9 ($|A - B|, B \subseteq A, |A| = \aleph_1, |B| = \aleph_0$) "Sejam A e B dois conjuntos, $B \subseteq A$. Se $|A| = \aleph_1$ e $|B| = \aleph_0$, então $|A - B| = \aleph_1$."

Suponha que $|A - B| = \aleph_0$. Então, de acordo com o Teorema 1.7, $|(A - B) \cup B| = \aleph_0$. No entanto, $(A - B) \cup B = A$ e, pela hipótese, $|A| = \aleph_1$. Portanto, $|A - B| \neq \aleph_0$. Por outro lado, como $A - B \subseteq A$, segue que $|A - B| \leqslant |A|$, ou seja, $|A - B| \leqslant \aleph_1$. Como $|A - B| \neq \aleph_0$, conclui-se que $|A - B| = \aleph_1$. □

O Teorema 1.10, apresentado a seguir, é uma versão modificada do Teorema 1.9.

Teorema 1.10 ($|A - B|, B \subseteq A, A$ é não enumerável e B é enumerável) "Sejam A e B dois conjuntos, $B \subseteq A$. Se A é não enumerável e B é enumerável, então $A - B$ é não enumerável."

Suponha que $A - B$ seja enumerável. Então, de acordo com o Teorema 1.7, $(A - B) \cup B$ é enumerável. No entanto, $(A - B) \cup B = A$ e, pela hipótese, A é não enumerável. Há, portanto, uma contradição, e disso resulta que $A - B$ é não enumerável. □

Exemplo 1.81 É sabido que $\mathbb{R}$ é não enumerável (ver Exemplo 1.73). Por outro lado, conforme o Exemplo 1.72, temos que $\mathbb{Q}$ é enumerável. Logo, o resultado acima (Teorema 1.10) prova que o conjunto dos números irracionais ($\mathbb{R} - \mathbb{Q}$) é não enumerável. ⋆

1.9 Exercícios

Conjuntos

1. Identifique, nas línguas portuguesa e inglesa, os conjuntos de letras, de palavras, de sentenças. Classifique-os em finitos ou infinitos. Estude as suas intersecções e uniões, indicando alguns dos elementos que pertencem a tais conjuntos, se existirem.
2. Para o conjunto $A = \{\emptyset, a, \{a\}\}$, calcule o conjunto potência $B = 2^A$, e então obtenha $A \times B, A \cup B$ e $A \cap B$.
3. Quais das expressões seguintes são verdadeiras?
   a) $\emptyset \subseteq \emptyset$
   b) $\emptyset \in \emptyset$
   c) $\emptyset \in \{\}$
   d) $\emptyset \in \{\emptyset\}$
   e) $\emptyset = \emptyset \cap \emptyset$
   f) $\{\emptyset\} \cap \emptyset = \emptyset$
   g) $\{\emptyset\} \cup \emptyset = \emptyset$
   h) $\{\emptyset\} - \emptyset = \emptyset$
4. Calcular os seguintes conjuntos:
   a) $(\{\} \cup \{a,b\} \cup \{\{a,b\}\}) - \{a,b\}$
   b) $2^{\{\}}$
   c) $\{a,b,c\} - (\{a\} \cup \{\{b,c\}\})$
   d) $2^{\{a,b,c\}} - 2^{\{a,c\}} - 2^{\{b\}}$
5. Provar as propriedades distributivas da operação de união em relação à de intersecção e da operação de intersecção em relação à de união de conjuntos.
6. Considere $A = \{m\}$ e $B = \{x,y\}$. Determine:
   a) $2^A \times 2^A$;
   b) 2^{2^A};

c) $B \times (A \times B)$;
d) $(B \times A) \times B$;
e) $2^{A \times B}$.

7. Determine $2^{\Sigma \times \Gamma}$ e $\Gamma \times (\Sigma \times \Gamma)$, para:
   a) $\Sigma = \{a\}$ e $\Gamma = \{b, c\}$;
   b) $\Sigma = \{a, b\}$ e $\Gamma = \{c\}$;
   c) $\Sigma = \{a, b\}$ e $\Gamma = \{c, d\}$.
8. Considere $\Sigma = \{0, 1\}, \Gamma = \{a, b, c\}$. Determine:
   a) Σ^*
   b) 2^{Γ}
   c) $\Sigma \times \Gamma$
   d) $\Sigma\Gamma$
9. Considere os conjuntos $A = \{\triangle, \square\}$, $B = \{1\}$ e $C = \{\alpha, \beta\}$, e determine:
   a) $C \times 2^{A \times B}$;
   b) $(A \cup 2^C) \times B$.
10. Considere os conjuntos $N = \{S, X\}$ e $\Sigma = \{a, b\}$, e determine:
    a) $\Sigma \times \Sigma$;
    b) $2^{\Sigma \times \Sigma}$;
    c) $2^{\Sigma} \times \Sigma$;
    d) $(N \times N) \times \Sigma$;
    e) $N \times (\Sigma \times \Sigma)$;
    f) $2^N \times 2^N$;
    g) N^2;
    h) $\Sigma^2 \times N$;
    i) $2^{\Sigma \times N}$;
    j) $\Sigma^3 N^2$.
11. Repita o Exercício 10 considerando:
    a) $N = \{S, X, Y\}$ e $\Sigma = \{a\}$;
    b) $N = \{S\}$ e $\Sigma = \{a, b, c\}$;
12. Considere $A = \{0, 1, 2\}, B = \{x, y\}, C = \{\#\}$ e calcule:
    a) $A \times B$
    b) $C \times B$
    c) $(A \times B) \times (C \times B)$
    d) 2^A
    e) 2^B
    f) 2^C
    g) $2^{(B \times C)}$
    h) $2^{(B \times C)} \times 2^A$
    i) $2^{(2^C)}$
    j) $2^{(2^C \times 2^B)}$
    k) $2^B \times 2^C$
    l) $(A \times B) \times 2^C$
    m) $A \times (B \times C)$
    n) $2^{(A \times B)} \times C$
    o) $2^{(2^{(B \times C)})}$
    p) $B \times 2^C$
    q) $2^{A \times (B \times C)}$
    r) $2^{(C \times 2^B)}$
    s) $2^A \times (2^B \times 2^C)$
    t) $(2^A \times 2^B) \times C$
    u) $B^2 C^3$
    v) 2^{B^2}
    w) $B^2 A \times C$
13. Seja A um conjunto qualquer. Determine:
    a) $2^{\emptyset}$
    b) $A \cup \emptyset$
    c) $A \cap \emptyset$
    d) $A - \emptyset$
    e) $\emptyset - A$
    f) $\overline{\emptyset}_A$
    g) $\overline{A}_{\emptyset}$
    h) $A \times \emptyset$

Relações

14. Para a relação $\{(a,b), (a,a), (b,a), (b,b), (b,c), (c,b), (c,c)\}$, qual é a sua relação inversa? Qual é o grafo que representa cada uma das duas relações?
15. Considere as operações relacionais apresentadas a seguir. Indique, para cada operação, se ela pode ser classificada como reflexiva, simétrica ou transitiva:
    a) $\neq$, sobre $\mathbb{N} \times \mathbb{N}$
    b) $\leqslant$, sobre $\mathbb{N} \times \mathbb{N}$
    c) $=$, sobre $\mathbb{N} \times \mathbb{N}$
    d) $>$, sobre $\mathbb{N} \times \mathbb{N}$
    e) $\subseteq$, sobre $2^{\mathbb{N}} \times 2^{\mathbb{N}}$
    f) $\supset$, sobre $2^{\mathbb{N}} \times 2^{\mathbb{N}}$

Funções

16. Descreva, sucintamente, a diferença entre os seguintes pares de conceitos:
    a) Produto cartesiano e concatenação
    b) Produto cartesiano e relação
    c) Relação e função
17. Quais são os atributos de uma função que permitem designá-la como sendo bijetora? Explique detalhadamente a caracterização de cada um desses atributos.
18. Conforme o modelo do Exemplo 1.44, identifique funções com características que permitam o preenchimento da tabela (I=Injetora, S=Sobrejetora, T=Total):

	I?	S?	T?
	Não	Não	Não
	Não	Não	Sim
$/ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$	Não	Sim	Não
$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$	Não	Sim	Sim
$\sqrt{} : \mathbb{Z} \to \mathbb{Z}$	Sim	Não	Não
	Sim	Não	Sim
	Sim	Sim	Não
	Sim	Sim	Sim

Grafos e árvores

19. Defina formalmente o que vem a ser um grafo.
20. O que significa dizer que um grafo é orientado, rotulado, ordenado ou cíclico?
21. Grafos não orientados podem eventualmente ser ordenados e/ou cíclicos? Justifique sua resposta.
22. Defina formalmente as particularidades que caracterizam um dado grafo como sendo uma árvore.

Teoremas e demonstrações

23. Provar, por indução, os seguintes resultados:
    a) A somatória dos n primeiros números ímpares positivos resulta no quadrado de n.
    b) O produto de n pela média dos extremos de uma progressão aritmética simples com n termos corresponde à soma de todos esses n termos.
    c) $\forall n \geqslant 0, (n-1)n^2(n+1)$ é sempre divisível por 3.
    d) $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1, n \geqslant 0$.
    e) $n! \geqslant 2^n, n \geqslant 4$.

Conjuntos enumeráveis

24. Responda às perguntas:
    a) O que é cardinalidade de um conjunto?
    b) O que é um conjunto enumerável (contável)?
    c) Formalmente, como é definido o conceito de conjunto infinito?
    d) Como podem ser comparadas as cardinalidades de dois conjuntos infinitos?
    e) Em que casos se pode afirmar que dois conjuntos quaisquer possuem a mesma cardinalidade?
25. Qual a importância do conceito de bijeção na definição de conjuntos enumeráveis?
26. Para um conjunto Σ finito não vazio, Σ^* é enumerável? Justifique sua resposta.
27. Considere o conjunto dos números naturais maiores ou iguais a cinco $(\{5,6,7,8,...\})$:
    a) Prove que esse conjunto é infinito.
    b) Prove que esse conjunto é enumerável.
28. Prove que o conjunto dos números naturais múltiplos de 10 $(\{0,10,20,...\})$ é um conjunto infinito.
29. Para os conjuntos seguintes, apresente, para os que forem enumeráveis, uma bijeção com os números naturais, ou então mostre que esta não existe:
    a) conjunto dos inteiros;
    b) conjunto dos reais positivos;
    c) conjunto dos múltiplos de 3;
    d) conjunto dos pontos do espaço tridimensional cujas coordenadas cartesianas são inteiras;
    e) conjunto dos pontos de um plano;
    f) conjunto dos pontos de intersecção das retas de uma malha plana bidimensional ortogonal cujas retas paralelas vizinhas distam 3 cm entre si;
    g) conjunto dos pontos da superfície de um cubo;
    h) conjunto dos números racionais;
    i) conjunto dos números complexos com componentes inteiras;
    j) conjunto dos números primos;
    k) subconjunto dos números naturais cuja representação decimal termine com um dígito que é primo;
    l) conjunto diferença entre o conjunto dos números reais positivos e o conjunto dos números naturais.

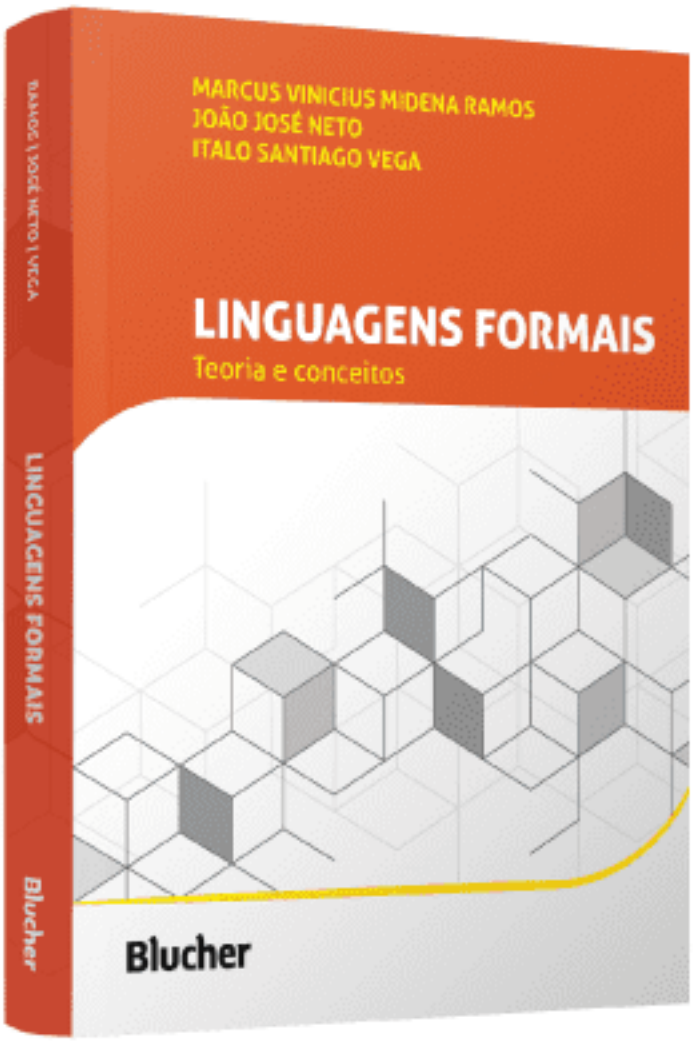
Concebido como referência para cursos superiores da área de computação, este livro explora tópicos sobre as linguagens definidas pela Hierarquia de Chomsky. Contudo, seu alcance foi expressivamente ampliado pela inclusão de introduções à matemática discreta, aos conceitos básicos de linguagens, à classe das linguagens recursivas, à análise sintática descendente, à decidibilidade e à complexidade.

Fruto de diversos anos da experiência docente e dedicação dos autores, em diversas instituições de ensino, à disciplina Linguagens Formais e Autômatos, esta obra, repleta de exemplos e exercícios, mitiga a aridez intrínseca dos muitos assuntos estudados, tornando-os mais acessíveis a um público-alvo amplo e diversificado.

ISBN 978-65-5506-716-3

www.blucher.com.br

Blucher



Clique aqui e:

VEJA NA LOJA

Linguagens formais

Teorias e conceitos

Marcus Vinicius Midena Ramos, João José Neto, Italo Santiago Vega

ISBN: 9786555067163

Páginas: 608

Formato: 17 x 24 cm

Ano de Publicação: 2023
