Matemática Discreta

José de Oliveira Guimarães
Campus de Sorocaba da UFSCar
Sorocaba - SP

19 de agosto de 2011

Sumário

Capítulo 1

Introdução

1.1 Afirmações, Teoremas e Semelhantes

Definição 1.1. Uma prova é uma derivação de uma afirmação a partir de hipóteses utilizando regras de dedução lógicas. A prova pode ser feita em uma lógica como a Lógica de Primeira Ordem ou usando uma linguagem natural.

Definição 1.2. Um axioma ou postulado é uma afirmação considerada evidente e que não necessita de prova.

Por exemplo, temos os cinco axiomas de Euclides sobre geometria Euclidiana. O primeiro deles diz que dois pontos definem uma única reta. O quarto diz que todos os ângulos retos são iguais.

Definição 1.3. Um teorema é uma afirmação que foi provada baseada em certas hipóteses. Um teorema é uma afirmação provada que possui certa importância.

Há afirmações que são provadas como um teorema mas que não possui a importância e a generalidade deste. Estas afirmações possuem muitos nomes:

Afirmação, Asserção, Resultado, Fato: uma afirmação prova sem muita importância. Geralmente utilizada na prova de um teorema ou proposição. Isto é, a prova consiste de vários "fatos", cada um deles provado separadamente;

Proposição: afirmação de importância intermediária entre um teorema e um resultado/fato;

Lema: uma afirmação utilizada na prova de um longo teorema. A prova do teorema é dividida em partes, sendo cada uma delas um Lema;

Corolário: um afirmação que tem uma prova curta baseada em um teorema ou proposição que está imediatamente antes;

A literatura matemática frequentemente utiliza outros nomes para afirmações provadas: identidade, regra, lei e princípio. Então podemos ter um "princípio da indução finita"que na verdade é um teorema em algumas situações.[1] E uma "lei" que é uma proposição.

[1] E axioma em outras!

Definição 1.4. Uma afirmação matemática que não foi provada é chamada de hipótese ou conjectura.

São exemplos de conjecturas:

conjectura de Goldbach: cada número par pode ser escrito como a soma de dois primos?

conjecture $3n + 1$**:** tome um número n. Se n é par, divida-o por 2. Se é ímpar, calcule $3n + 1$. Repita o processo. Para qualquer número n chegaremos a 1?

primos gêmeos: há infinitos primos da forma p e $p + 2$?

1.2 Linguagem Lógica de Primeira Ordem

Neste livro usaremos algumas fórmulas lógicas expressas na linguagem da lógica de primeira ordem (LPO). Definiremos informalmente então o que é uma fórmula nesta linguagem. Outros conceitos desta lógica necessários a este texto podem ser encontrados em Guimarães [6].

Uma linguagem da LPO é associada a um vocabulário, que é uma tripla formada por um conjunto de símbolos de predicado, um conjunto de símbolos de função e um conjunto de símbolos de constantes. A linguagem define o que é uma fórmula válida.

A linguagem da lógica de primeira ordem utiliza o alfabeto

$$\{\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow, \forall, \exists, (,)\} \cup \{x_1, x_2, \ldots\} \cup \Sigma \cup \Delta \cup \Psi$$

no qual x_i é uma variável, $i \in \mathbb{N}$, Σ é um conjunto de símbolos de predicado, Δ é um conjunto de símbolos de função e Ψ um conjunto de símbolos de constantes. Usamos meta-variáveis x, y, z, etc. Uma meta-variável representa e pode ser substituída por uma variável qualquer (x_i ou outra meta-variável).

Definição 1.5. Um **termo** é definido indutivamente como

1. uma variável ou constante é um termo;
2. se f é um símbolo de função que toma n argumentos (n-ário) e t_1, t_2, ... t_k são termos, então $f(t_1, t_2, ..., t_n)$ é um termo. Observe que um símbolo de função de aridade[2] n deve ser utilizado com n termos.

Um vocabulário apropriado para fórmulas sobre os números naturais é $\mathcal{V} = (\{<, \leqslant\}, \{+, \cdot\}, \{0, 1\})$. $<$ e $\leqslant$ são símbolos de predicado, $+$ e $\cdot$ são símbolos de função binários e 0 e 1 são constantes. A linguagem $\mathcal{L}_A$ associada a este vocabulário possui termos como

1. 0, 1, x_1, x_7, x_i para $i \in \mathbb{N}$;

[2] A aridade de uma função é o número de argumentos que ela exige.

2. $0 + x_1$, $(0 + 0) + 1$

3. $x \cdot (y + z)$, usamos meta-variáveis aqui;

4. $+(x, y)$, $\cdot(+(1, x), y)$, usamos a notação usual de função para + e $\cdot$

Definição 1.6. Uma **fórmula atômica** é definida indutivamente como:

- $t_1 = t_2$, com t_1 e t_2 termos de $\mathcal{L}$ ou;
- $P(t_1, t_2, ..., t_n)$ sendo que P é um símbolo de predicado n-ário pertencente a Σ e t_1, t_2, ..., t_n são termos.

Definição 1.7. Uma fórmula da linguagem de primeira ordem é definida como

1. toda fórmula atômica é fórmula;

2. se A e B são fórmulas e x é uma variável qualquer, então $(\neg A)$, $(A \vee B)$, $(A \wedge B)$, $(A \longrightarrow B)$, $(A \longleftrightarrow B)$, $((\forall x)A)$ e $((\exists x)A)$ são fórmulas. O símbolo $\exists$ é chamado de *quantificador existencial* e $\forall$ é o *quantificador universal*;

3. nada mais é uma fórmula.

Usamos A, B, C, ... para meta-fórmulas. Uma meta-fórmula representa uma fórmula qualquer. A precedência dos operadores é a seguinte, do maior para o menor: $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$, $\longrightarrow$, $\longleftrightarrow$. Os quantificadores $\forall$ e $\exists$ têm a mesma precedência. Não utilizaremos parênteses a não ser que haja alguma ambigüidade.

1.3 Conceitos e Equivalências Lógicas Importantes

Apresentamos abaixo algumas equivalências lógicas importantes. Usamos $A \equiv B$ para A é logicamente equivalente a B.

1. Usamos a notação $\Gamma \models A$ para representar que A é conseqüência lógica do conjunto de fórmulas Γ. Isto é, sempre que todas as fórmulas de Γ forem verdadeiras, A será verdadeiro.[3] Se $\Gamma = \{B\}$, usamos $B \models A$. Neste texto, Γ estará implícito, será o conjunto de axiomas da Matemática adequado para cada caso. Você pode considerá-lo como o conjunto dos seus conhecimentos matemáticos sobre o assunto;

2. $A \longleftrightarrow B \equiv (A \longrightarrow B) \wedge (B \longrightarrow A)$. Isto é, $\Gamma \models A \longleftrightarrow B$ sse $\Gamma \models (A \longrightarrow B) \wedge (B \longrightarrow A)$

3. $A \longrightarrow B \equiv \neg B \longrightarrow \neg A$. Isto é, $\Gamma \models A \longrightarrow B$ sse $\Gamma \models \neg B \longrightarrow \neg A$

[3] No Cálculo Proposicional. Na LPO, A deve ser verdadeira em todos os modelos de Γ.

4. prova por contradição. Considere que $\perp$ é uma contradição, por exemplo, $A \wedge \neg A$. Se $\Gamma \vDash \neg A \longrightarrow \perp$ então $\Gamma \vDash A$. Pela tabela verdade de $\longrightarrow$, como $\neg A \longrightarrow \perp$ é considerada V (verdadeiro) quando Γ o for, então $\neg A$ só pode ser F (se fosse V, teríamos V $\longrightarrow$ F, o que é F — mas assumimos que $\neg A \longrightarrow \perp$ é V). Como $\neg A$ é F, A é V, verdadeiro.

   Para provar A, assumimos $\neg A$ e chegamos a uma contradição. Então podemos afirmar que A é verdadeira;

5. $\neg(A \longrightarrow B) \equiv \neg(\neg A \vee B) \equiv A \wedge \neg B$. Para provar $A \longrightarrow B$, podemos negar esta fórmula, tentar fazer a prova e chegar a uma contradição. Então tentamos provar $\neg(A \longrightarrow B)$. Ao encontrar uma contradição, temos que $A \longrightarrow B$ é verdadeira. Contudo, em geral não tentamos provar $\neg(A \longrightarrow B)$ e sim uma fórmula logicamente equivalente a ela, $A \wedge \neg B$.

6. $A \longleftrightarrow B \equiv (A \longrightarrow B) \wedge (\neg A \longrightarrow \neg B)$. Em uma prova "$A$ sse B", podemos provar que: a) A implica B e b) se A é falso então B é falso (não A implica não B).

1.4 Nomenclatura Matemática

(a) Escrevemos $A \Longrightarrow B$ para "se A então B". Esta frase é lida como "A é suficiente para B"ou "B é necessário para A". O fato de A ser verdadeiro é suficiente para B ser verdadeiro também. O fato de B ser verdadeiro é necessário para A ser verdadeiro; isto é, A não pode ser verdadeiro sem que B também o seja. Quando "A é necessário e suficiente para B", então temos A se e somente se B;

(b) Usamos **sse** como abreviatura para "se e somente se";

(c) frequentemente, nas provas, não colocamos "para todo x" ou "para todo n". O "para todo" fica implícito. Por exemplo, escrevemos

   se $n > 3$ é primo, então $n + 1$ não é primo. Queremos dizer "para todo n, se $n > 3$ primo, $n + 1$ não é primo".

   Nas provas, freqüentemente se usa "dado x ..." isto quer dizer "para todo x de certo domínio ...".

1.5 Tipos de Provas

Esta seção apresenta os tipos de prova mais comuns. Normalmente, ao fim de uma prova coloca-se um quadrado cheio ■, vazio □ ou QED. Este último é uma abreviação de Quod Erat Demonstrandum, uma frase em Latin que significa "o que era para ser demostrado".

1.5.1 Prova Direta

Neste tipo de prova tem-se que provar uma afirmação do tipo $A \longrightarrow B$ e usa-se o fato A para provar B diretamente.

Proposição 1.1. *Se $n \in \mathbb{N}$ é par, n^2 é par.*

Demonstração. Par é todo número inteiro que pode ser escrito da forma $2k$ para algum $k \in \mathbb{Z}$. Como n é par, $n = 2k$. Então $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Logo n^2 é par. □

1.5.2 Prova por contrapositiva

Este tipo de prova se baseia na equivalência lógica $A \longrightarrow B \equiv \neg B \longrightarrow \neg A$.

Proposição 1.2. *Para $n \in \mathbb{N}$, se n^2 é par, então n é par.*

Demonstração. Provaremos a contrapositiva, isto é, "se n não é par, então n^2 não é par" ou "se n é ímpar, então n^2 é ímpar".

Como n é ímpar, $n = 2m + 1$ para $m \in \mathbb{N}$, $m \geqslant 0$. Então

$$n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$$

que é ímpar. □

1.5.3 Prova por Contradição

Para provar que alguma afirmação P é verdadeira, podemos supor que o contrário é que é verdadeiro; ou seja, "não P". Se encontrarmos uma contradição durante a prova, então é certo que assumimos algo falso como premissa. No caso, "não P" é falso, o que significa que P é verdadeiro (não não P é igual a P). Vejamos um exemplo.

Definição 1.8. Um número x é racional se pode ser escrito como uma razão de inteiros a e b, com $b \neq 0$. Isto é, $x = \frac{a}{b}$.

Proposição 1.3. *Provar que $\sqrt{2}$ é irracional.*

Demonstração. Suporemos que $\sqrt{2}$ é número racional. Então existem dois inteiros a e b tal que $\sqrt{2} = \frac{a}{b}$. Podemos assumir também, sem perda de generalidade, que a e b não têm fatores em comum (isto é, não há um número inteiro que divide ambos).

Sendo $\sqrt{2} = \frac{a}{b}$, temos que $2 = \frac{a^2}{b^2}$ e $2b^2 = a^2$. Então a^2 é um número par, pois é da forma $2p$, sendo que $p = b^2$. Sendo a^2 par, então a é par e portanto pode ser escrito como $2q$. Isto é, $a = 2q$. Logo, $2b^2 = (2q)^2$, $2b^2 = 4q^2$ e $b^2 = 2q^2$, o que implica que b^2 é par e portanto b é par. Contradição, pois agora ambos, a e b são divisíveis por 2, sendo que assumimos que estes números não têm divisores em comum.

Logo podemos concluir que a hipótese inicial, que $\sqrt{2}$ é racional, é falsa. Logo $\sqrt{2}$ é irracional. □

1.5.4 Prova por Casos

Algumas vezes uma prova deve ser dividida em diversas partes e cada uma delas deve ser provada separadamente.

Proposição 1.4. *Prove que, dados n e m naturais, n e m têm a mesma paridade (ambos pares ou ambos ímpares) se e somente se n + m é par.*

Demonstração. A proposição é da forma $A \longleftrightarrow B$ pois é um "se e somente se". Então temos que provar $A \longrightarrow B$ e $B \longrightarrow A$. Ou, equivalentemente, $A \longrightarrow B$ e $\neg A \longrightarrow \neg B$. Ou seja, provaremos que a) se n e m têm a mesma paridade, $n + m$ é par e b) se n e m não têm a mesma paridade, $n + m$ não é par (é ímpar). Há quatro casos a considerar, dois para cada item a) e b):

(a) n par e m par: $n = 2k$, $m = 2t$, $n + m = 2(k + t)$ e portanto par;

(b) n ímpar e m ímpar: $n = 2k + 1$, $m = 2t + 1$, $n + m = 2(k + t) + 2 = 2(k + t + 1)$ e portanto par;

(c) n ímpar e m par: $n = 2k + 1$, $m = 2t$, $n + m = 2(k + t) + 1$, ímpar;

(d) n par e m ímpar: $n = 2k$, $m = 2t + 1$, $n + m = 2(k + t) + 1$, ímpar.

□

1.5.5 Prova por Contra-Exemplo

Dada uma afirmação qualquer, podemos refutá-la encontrando um exemplo que torna a afirmação falsa. Por exemplo, "todos os primos são ímpares". Para refutar esta afirmação, basta encontrar um primo que é par. 2 é primo e é par. Logo a afirmação é falsa. Isto é, a afirmação "Há pelo menos um primo que é par" é verdadeira.

Há um outro método de prova que será utilizado neste livro. É a chamada "prova por intimidação" em que o autor simplesmente escreve "trivial" no espaço reservado à prova. É um tipo de prova fácil de fazer e no qual os erros são impossíveis.[4]

Exercícios

1.1. O que é um teorema? E um lema? Uma conjectura é uma hipótese?

1.2. Cite uma conjectura famosa da Matemática não citada neste Capítulo.

1.3. Explique com as suas palavras as equivalências lógicas dadas neste Capítulo.

1.4. Prove que, se n^2 é múltiplo de 3, n é múltiplo de 3.

[4]Este método possui inúmeras vantagens, mas não pode ser utilizado em nenhuma avaliação.

1.5. Prove que $\sqrt{3}$ é irracional.

1.6. Prove que, se $x_1, x_2 \in \mathbb{R}^+$, então

$$\sqrt{x_1 x_2} \leqslant \frac{x_1 + x_2}{2}$$

Generalize esta fórmula para n variáveis (**difícil**).

1.7. Prove, sem utilizar indução finita:

(a) se $a_{i+1} = a_i + c$ e $S_n = a_1 + a_2 + \ldots + a_n$, então

$$S_n = \frac{(a_1 + a_n)n}{2}$$

(b) seja $S_n = a + aq + aq^2 + \ldots + aq^{n-1}$, $q \neq 1$. Então

$$S_n = \frac{a(q^n - 1)}{q - 1}$$

(c) seja $S_n = a + aq + aq^2 + \ldots$ com $q < 1$ — uma série infinita. Então

$$S_n = \frac{a}{1 - q}$$

1.8. A soma de dois racionais é racional? A soma de dois irracionais é irracional? A soma de um racional com um irracional pode ser racional? O produto de dois irracionais pode ser racional? O produto de um irracional por um racional pode ser racional? A divisão de um irracional por outro irracional pode ser racional?

Capítulo 2

Indução Finita e Definição por Indução

Teorema 2.1. *Considere uma afirmação $A(n)$ onde $n \in \mathbb{N}$; isto é, A é parametrizada por um número natural n. Se provarmos*

(a) *A para um caso base $A(b)$ onde $b \in \mathbb{N}$ e;*

(b) *que $A(n)$ implica em $A(n+1)$*

então teremos provado $A(n)$ para todo $n \in \mathbb{N}$, $n \geqslant b$. Este é o chamado **Princípio da Indução Finita***, que na verdade é um teorema.*

Colocando este teorema em notação lógica, temos

$$A(b) \wedge \forall n(A(n) \longrightarrow A(n+1)) \longrightarrow \forall n(n \geqslant b \longrightarrow A(n))$$

De fato, o teorema da indução finita é mais geral do que esta fórmula lógica por razões que serão explicadas futuramente (se forem explicadas). Este teorema pode ser deduzido do axioma da boa ordenação dos números naturais que diz que qualquer subconjunto de $\mathbb{N}$ tem um menor elemento. De fato, o axioma e o teorema acima são equivalentes.

Em uma demonstração por indução, utilizamos a seguinte nomenclatura:

a demonstração de $A(b)$ é chamada de **caso base**;

$A(n)$ é chamada de **hipótese de indução**. É um fato que supomos verdadeiro para provar $A(n+1)$.

A demonstração da implicação $A(n) \longrightarrow A(n+1)$ é chamada de **passo da indução**.

O princípio da indução finita pode ser descrito em termos de conjuntos da seguinte forma [5].

Teorema 2.2. *Seja $n_0 \in \mathbb{N}$ e S um conjunto tal que:*

(a) *$n_0 \in S$;*

(b) *se $s \in S$ então $s \geqslant n_0$;*

(c) *se $n \in S$ então $n + 1 \in S$;*

então $S = \{n : n \in \mathbb{N}$ e $s \geqslant n_0\}$.

Nem sempre assumimos que $A(n)$ é válido (HI) para provar $A(n + 1)$. Quando for conveniente, podemos assumir que $A(n - 1)$ é válido e então provar $A(n)$.

O teorema da indução finita acima pode ser provado utilizando-se outros teoremas da Matemática, o que não será feito aqui.

Vamos estudar um exemplo.

Proposição 2.1.

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Demonstração. Considere $S_n = 1 + 2 + 3 + \ldots + n$, então $S_n = \frac{n(n+1)}{2}$.

Para $n = 1$, $S_1 = 1$ e $S_1 = \frac{1(1+1)}{2} = 1$, o que prova a hipótese.

Suponha que a hipótese seja válida para $n - 1$, isto é,

$$S_{n-1} = \frac{(n-1)(n-1+1)}{2} = \frac{(n-1)n}{2} = 1 + 2 + \ldots + (n-1)$$

Provaremos que ela é válida para S_n. Sendo $S_n = S_{n-1} + n$, então

$$S_n = \frac{(n-1)n}{2} + n = \frac{(n^2 - n + 2n)}{2} = \frac{n(n+1)}{2}$$

o que prova a hipótese. Neste exemplo, a HI é $S_n = \frac{n(n+1)}{2}$.

□

Proposição 2.2.

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Demonstração. Para o caso base tomamos $n = 0$. Então

$$\sum_{i=0}^{0} 2^i = 2^0 = 1 \tag{2.1}$$

$$2^{0+1} - 1 = 2^1 - 1 = 1 \tag{2.2}$$

$$\tag{2.3}$$

Assuma que a HI é válida; isto é,

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Então

$$\sum_{i=0}^{n+1} 2^i = (\sum_{i=0}^{n} 2^i) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2.2^{n+1} - 1 = 2^{n+2} - 1$$

□

Proposição 2.3. *Considere n retas distintas no plano. Estas retas dividem o plano em um certo número de regiões delimitadas por segmentos de retas ou retas. Dentro de uma região não há nenhuma reta ou segmento de reta. Por exemplo, uma única reta delimita o plano em duas regiões. Duas retas paralelas dividem o plano em três regiões e duas retas que se cruzam dividem o plano em quatro regiões.*

Uma coloração válida para um plano com n retas associa uma cor para cada região de tal forma que duas regiões com um segmento de reta em comum não tenham a mesma cor.

Prove que existe uma coloração válida para um plano com qualquer número de retas que utiliza apenas duas cores.

Demonstração. Provaremos por indução finita. Claramente, para $n = 1$ duas cores são suficientes. Considere agora a afirmação válida para $n - 1$ retas. Iremos provar que ela é válida também para n retas.

Considere o plano com n retas. Remova uma reta. Pela HI, é possível colorir o plano com duas cores. Agora acrescente a reta que foi removida e inverta as cores em um dos semi-planos definido pela reta (e apenas em um deles). As regiões que estão em apenas um dos lados da reta continuam com a coloração válida — as cores em regiões separadas por uma reta ou segmento de reta continuam diferentes. As regiões divididas ao meio pela n-ésima reta, adicionada, são coloridas por duas cores diferentes também. Logo a coloração para n retas também é válida. □

O princípio da indução finita (Teorema 2.2) apresentado acima é chamado de **princípio da indução fraca**. Há um outro teorema, o da indução forte. Este teorema assume como hipótese de indução que a afirmação $A(n)$ é válido para $k < n$.

Teorema 2.3. *Princípio da indução finita forte: considere uma afirmação $A(n)$ onde $n \in \mathbb{N}$. Se provarmos*

(a) *que $A(b)$ é verdadeira no qual $b \in \mathbb{N}$ e;*

(b) *que $A(n)$ é verdadeira assumindo que $A(k)$ é verdadeira para $b \leqslant k < n$*

então teremos provado $A(n)$ para todo $n \in \mathbb{N}$, $n \geqslant b$. Colocando esta afirmação em notação lógica, temos

$$A(b) \wedge \forall n((\forall k\,(b \leqslant k \wedge k < n \longrightarrow A(k))) \longrightarrow \forall n(b \leqslant n \longrightarrow A(n))$$

De fato, os dois tipos de indução são equivalentes.

Teorema 2.4. *O teorema da indução finita fraca implica o teorema da indução finita forte e vice-versa.*

Proposição 2.4. *Você tem uma quantidade ilimitada de selos de* 3 *e* 5 *centavos. Prove que, com estes selos, você pode selar qualquer correspondência com o valor exato, desde que este valor seja maior do que* 8 *centavos.*

Demonstração. Em outras palavras, todo número $n \geqslant 8$, $n \in \mathbb{N}$, é tal que $n = 3a + 5b$, onde $a, b \in \mathbb{N}$.

O caso base é $n = 8 = 3 + 5$.

A HI é "para $8 \leqslant k < n$, existem a e b em $\mathbb{N}$ tal que $k = 3a + 5b$".

Faremos a prova de que n pode ser expresso como $3a' + 5b'$ por partes:

- $n = 9$. Neste caso, $n = 3 \cdot 3 + 5 \cdot 0$
- $n = 10$. Neste caso, $n = 3 \cdot 0 + 5 \cdot 2$
- $n > 10$. Neste caso, $n - 3 = 3a + 5b$ com $a, b \in \mathbb{N}$, pela HI, pois $8 \leqslant n - 3 < n$. Então $n = 3(a + 1) + 5b$, com $a + 1, b \in \mathbb{N}$.

Logo a proposição está provada. □

Antes de mostrar o próximo exemplo, o leitor é convidado a ler o apêndice C sobre Grafos.

Proposição 2.5. *O número n de vértices de uma árvore binária cheia (zero ou dois filhos) é ímpar.*

Demonstração. O caso base é $n = 1$. Trivial.

Suponha que o número de vértices k de uma ABCh seja ímpar para $1 \leqslant k < n$ (HI).

Tome a árvore com n vértices, $n > 1$. Sejam C e D as suas sub-árvores. O número de vértices de C (ou D) é menor do que n. E cada sub-árvore tem um número ímpar de vértices pela HI. O número de vértices da árvore completa é 1 + dois números ímpares. Portanto, um número ímpar. □

Note que não sabemos o número de vértices de C ou D. Não importa. O que interessa é que este número é menor do que n. Neste caso obrigatoriamente temos que utilizar o princípio da indução forte.

Proposição 2.6. *O número de folhas de uma árvore binária cheia com n vértices é* $\frac{n+1}{2}$.

Demonstração. O caso base é $n = 1$. O número de folhas é $1 = \frac{1+1}{2}$. Confere.

A HI é "para AB com k vértices, $1 \leqslant k < n$, o número de folhas é $\frac{k+1}{2}$.

Considere uma AB com n vértices, $n > 1$, na qual a raiz é ligada a sub-árvores C e D (sempre temos C e D pois $n > 1$ e a árvore é cheia). O número de folhas da árvore é o número de folhas de C mais o número de folhas de D. Suponha que o número de vértices de C e D sejam k e m, respectivamente. Então o número de folhas de cada sub-árvore, aplicando a HI, é $\frac{k+1}{2}$ e $\frac{m+1}{2}$. Então o número de folhas da AB é

$$\frac{k+1}{2} + \frac{m+1}{2} = \frac{(k+m+1)+1}{2} = \frac{n+1}{2}$$

Observe que $n = k + m + 1$. □

Novamente utilizamos o princípio da indução forte. Não sabemos o número de vértices de C ou D. Sabemos apenas que é menor do que n.

É muito importante notar que só podemos utilizar a HI se o problema para números $< n$ são da mesma natureza que o problema original. No caso acima, utilizamos a HI para as sub-árvores C e D. Mas para isto C e D devem satisfazer a hipótese original; isto é, C e D devem ser **árvores binárias cheias**. Será que são? Claramente sim. Se C, por exemplo, não fosse árvore binária cheia, ela teria um vértice com um único filho. Então a árvore original também teria um vértice com um único filho e não seria cheia. Mas a hipótese da proposição é que a árvore é cheia.

Vejamos um exemplo, incompleto, que mostra que não podemos aplicar descuidadamente a HI para números menores do que n. Queremos provar uma proposição $A(n)$ para um grafo não dirigido conectado G, onde n é o número de vértices. Um grafo é conectado se há um caminho entre dois vértices quaisquer. Então a HI exige que $A(n)$ só se aplique a grafos conectados. Depois de provar o caso base, $n = 1$, retiramos um vértice v do grafo G, juntamente com as arestas adjacentes a ele, e aplicamos a HI.

Mas isto está errado. Só se pode aplicar a HI a grafos conectados. E o grafo G sem v pode ser desconectado. Então não podemos retirar um vértice qualquer. Tem que ser um vértice que, removido, não desconecta o grafo. Possivelmente um vértice v que está ligado a um único outro vértice. Ou retiramos um v qualquer, mas aplicamos a HI a todos os sub-grafos resultantes que são conectados. Para imaginar esta última situação, imagine três grafos "triângulo"[1] não conectados entre si. Agora acrescente um vértice v e o ligue a um e apenas um vértice de cada um dos triângulos. O grafo resultante é G. Na proposição acima, se retirarmos v para aplicar a HI, temos que aplicá-la a todos os três triângulos. Observe que, ao remover o vértice, removemos também as arestas ligadas a ele.

Definição 2.1. O mesmo mecanismo de prova por indução pode ser aplicado a **definições** resultando em **definição por indução**. Para definir um objeto indutivamente, especificamos

(a) um caso base que não utiliza a própria definição do objeto;

(b) um passo indutivo que mostra como construir o objeto baseado em instâncias menores do próprio objeto.

Este tipo de definição é chamado definição por indução.

Exemplo 2.1. Uma sequência de Fibonacci é definida indutivamente como: $f(1) = f(2) = 1$ (caso base) e $f(n) = f(n-1) + f(n-2)$. O caso base é $f(1) = f(2) = 1$ e o passo indutivo é a definição $f(n) = f(n-1) + f(n-2)$.

Exemplo 2.2. Dado $n \in \mathbb{N}$, n' é o elemento sucessor de n. Baseado nesta operação, podemos definir indutivamente a soma de dois naturais: $n + 0 = n$ (caso base) e $n + m' = (n + m)'$

[1] Um grafo com três vértices, cada um ligado a dois outros.

Exemplo 2.3. Dado um conjunto Σ finito de elementos, define-se *cadeia sobre* Σ indutivamente da seguinte forma:

(a) ϵ, a cadeia vazia, composta por zero elementos, é uma cadeia;

(b) se w é uma cadeia e $s \in \Sigma$, então sw é uma cadeia.

A junção de dois ou mais símbolos (colocados lado a lado) é a operação de concatenação. Por exemplo, se $\Sigma = \{0, 1\}$, pode-se concatenar 0 e 1 formando-se 01. A concatenação de ϵ com w qualquer é w.

Então são cadeias sobre $\Sigma = \{0, 1\}$: $\epsilon, 0, 1, 00, 01, 10, 11, 000, \ldots$. O conjunto de todas estas cadeias é denotado por $\Sigma^\star$.

Exemplo 2.4. Em lógica, as fórmulas do cálculo proposicional são definidas indutivamente como

(a) uma variável V_i, $i \in \mathbb{N}$, é uma fórmula;

(b) $\neg A$ e $(A \vee B)$ são fórmulas se A e B são fórmulas;

Um certo objeto é definido se, partindo dos casos base (pode haver mais de um), pode-se construi-lo em um número finito de passos a partir dos passos da definição por indução. Por exemplo, $(V_3 \vee \neg V_2) \vee V_2$ é uma fórmula porque:

1. V_1, V_2 e V_3 são fórmulas pelo caso base (a);
2. $\neg V_2$ é fórmula porque V_2 é fórmula e a negação de uma fórmula é fórmula (passo (b));
3. $(V_3 \vee \neg V_2)$ é fórmula porque V_3 e $\neg V_2$ são fórmulas;
4. como $(V_3 \vee \neg V_2)$ e V_2 são fórmulas, pelo passo da indução (b) então $(V_3 \vee \neg V_2) \vee V_2$ é fórmula.

Exercícios

2.1. Prove por indução:

(a) $2^n < n!$ para $n \geqslant 4$;

(b) $(1 + x)^n \geqslant 1 + nx$;

(c) para todo k, existe n_0 tal que para $n \geqslant n_0$, $n^k < 2^n$;

(d)

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

(e) $x^n - y^n$ é divisível por $x - y$ para todos os números naturais x, y, n;

(f)
$$\sum_{j=1}^{n}(2j-1) = 1 + 3 + 5 + \ldots + (2n-1) = n^2$$

(g) para todo $n \in \mathbb{N}$, $9^n - 1$ é divisível por 8;

(h) se $a_{i+1} = a_i + c$ e $S_n = a_1 + a_2 + \ldots + a_n$, então
$$S_n = \frac{(a_1 + a_n)n}{2}$$

(i) seja $S_n = a + aq + aq^2 + \ldots + aq^{n-1}$, $q \neq 1$. Então
$$S_n = \frac{a(q^n - 1)}{q - 1}$$

(j) $9^n - 1$ é divisível por 8 para todo $n \in \mathbb{N}$.

2.2. Prove por indução que o programa abaixo calcula o fatorial do seu argumento. É um exercício trivial, mas que ajuda a relacionar indução finita com algoritmos recursivos.

```
int fatorial(int n) {
  if ( n == 0 )
     return 1;
  else
     return n*fatorial(n-1);
}
```

2.3. De quantos modos diferentes podemos colocar $n + 1$ bolas em n caixas?

2.4. Prove que o número de subconjuntos de um conjunto de $n \in \mathbb{N}$ elementos é 2^n.

2.5. Encontre uma fórmula para a seguinte soma e prove por indução que ela está correta.
$$1 \cdot 2 + 2 \cdot 3 + \ldots + n(n+1)$$

2.6. Coloque o princípio da indução finita forte em termos de conjuntos.

2.7. (Dificuldade média) Prove o Teorema 2.4.

2.8. Prove por indução que o número de vértices de uma ABC de altura h é $2^h - 1$.

2.9. Prove por indução que o número de folhas de uma ABC de altura h é 2^{h-1}.

2.10. Prove por indução que uma árvore com n vértices tem $n - 1$ arestas.

2.11. Dê uma definição indutiva de `struct`´s da linguagem C++.

2.12. Considere a seguinte definição indutiva de tipos:

(a) `int` e `bool` são tipos;

(b) se α_i, $1 \leqslant i \leqslant n$ são tipos, então $(\alpha_1 \times \alpha_2 \times \ldots \alpha_n)$ e $(\alpha_1 \times \alpha_2 \times \ldots \alpha_n \longrightarrow \beta)$ são tipos;

Assuma que parenteses possam ser removidos se nenhuma ambiguidade é introduzida. Baseado nesta definição, responda:

(a) são `int` $\times$ `int` $\longrightarrow$ `int` e `int` $\longrightarrow$(`bool` $\times$ `bool` $\longrightarrow$ `bool`) tipos?

(b) faça todos os passos a partir do caso base da definição de um tipo que corresponde a uma função que toma um inteiro e um valor booleano como parâmetros e retorna dois inteiros.

Capítulo 3

Introdução à Teoria dos Números

A teoria dos números estuda as propriedades dos números inteiros, o conjunto $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$. Neste curso estudaremos a divisibilidade, os números primos, o máximo divisor comum, o teorema fundamental da Aritmética e relações de congruência.

Usaremos $\mathbb{N}$ para os números naturais $0, 1, 2, \ldots$ e $\mathbb{N}^\star$ para $\{1, 2, 3, \ldots\}$ (os naturais sem o zero).

Proposição 3.1. *Para cada $n \in \mathbb{N}$ e cada $d \in \mathbb{N}^\star$ existem e são únicos os números $q, r \in \mathbb{N}$ tais que*

$$n = dq + r$$

com $0 \leqslant r < d$.

Demonstração. antes de fazer as provas, mostraremos o algoritmo para calcular q e r. Estudando-o, a prova abaixo se torna mais fácil de compreender.

```
// entrada: n e d
q = 0;
while (d*(q + 1) <= n) do
   q = q + 1;
r = n - dq;
```

Se o laço não é executado nenhuma vez, temos $q = 0$ e $d > n$. Neste caso, $r = n$ e $r < d$. Se o laço executa pelo menos uma vez, ao final da instrução `q = q + 1` do `while` temos sempre $dq \leqslant n$. Quando o laço termina, após uma instrução $q = q + 1$, $d(q + 1) > n$. Então

$$\begin{array}{lll} dq & \leqslant n & < d(q+1) \\ dq - dq & \leqslant n - dq & < d(q+1) - dq \\ 0 & \leqslant r & < d \end{array}$$

Há duas provas a fazer: existência e unicidade. Primeiro provaremos a existência por indução finita.

O caso base é $n = 0$. Neste caso, use $q = r = 0$. Considere agora $n > 0$. Então pela HI existem q e r tais que $n = dq + r$ com $0 \leqslant r < d$. Encontraremos q' e r' para a divisão de $n + 1$ por d.

Se $r+1 < d$, basta tomar $q' = q$ e $r' = r+1$ pois $n+1 = dq+r+1 = dq+(r+1)$. Se $r+1 = d$,

$$n+1 = dq+r+1 = dq+d = d(q+1)+0$$

Tomamos $q' = q+1$ e $r' = 0$.

Provaremos a unicidade. Suponha que $n = dq+r = d\overline{q}+\overline{r}$. Logo $d(q-\overline{q}) = \overline{r}-r$ e

$$|d|\left|(q-\overline{q})\right| = \left|\overline{r}-r\right|$$

Como $0 \leqslant r < d$ e $0 \leqslant \overline{r} < d$, temos $0 \leqslant \left|\overline{r}-r\right| < d$. Por $|d|\left|(q-\overline{q})\right| = \left|\overline{r}-r\right|$ e $0 \leqslant \left|\overline{r}-r\right| < d$, deduzimos que $0 \leqslant \left|q-\overline{q}\right| < 1$ e $\left|q-\overline{q}\right| = 0$. Logo $q = \overline{q}$. Por $|d|\left|(q-\overline{q})\right| = \left|\overline{r}-r\right|$ e $q = \overline{q}$ deduzimos $r = \overline{r}$.

□

Proposição 3.2. *Para cada $n \in \mathbb{Z}$ e cada $d \in \mathbb{Z}, d \neq 0$, existem e são únicos os números $q \in \mathbb{Z}$ e $r \in \mathbb{N}$ tais que*

$$n = dq+r$$

com $0 \leqslant r < |d|$.

Definição 3.1. Dados $n, m \in \mathbb{Z}$, dizemos que m divide n se existe $k \in \mathbb{Z}$ tal que $n = km$. Neste caso usamos a notação $m|n$. Se $m \neq 0$, dizemos que n é divisível por m. Neste caso, o resto da divisão de n por m é zero.

Exemplo 3.1. $0 = 1.0$ Logo $0|0$.
$0 = 0n$ para todo $n \in \mathbb{Z}$. Logo $n|0$.
$6 = 2 \cdot 3$ e $6 = 3 \cdot 2$. Logo $3|6$ e $2|6$.

Definição 3.2. Um número $n \in \mathbb{Z}$ é chamado de *par* se $n = 2q$ para algum $q \in \mathbb{Z}$ (o resto da divisão de n por 2 é 0). Um número $n \in \mathbb{Z}$ é *ímpar* se $n = 2q+1$ para algum $q \in \mathbb{Z}$ (o resto da divisão de n por 2 é 1).

Proposição 3.3. *Proposições sobre divisibilidade. São apresentadas provas sumárias dos itens (b) e (c).*

(a) se $n = km$, $m|n$ e $k|n$;

(b) se $m|n$ e $n|p$, então $m|p$. Temos $n = km$ e $p = k'n$. Logo $p = k'km$ e $m|p$.

(c) se $m|n$ e $m|p$, então $m|(tn+up)$, para todo $t, u \in \mathbb{Z}$. Temos $n = km$ e $p = k'm$ e $tn = tkm$, $up = uk'm$, $tn+up = tkm+uk'm = (tk+uk')m$. Portanto $m|(tn+up)$.

Uma prova errada do item (b) seria: $n = km$, $p = kn$ e então $p = k(kn) = k^2n$. Isto está errado porque não se considerou p e n em toda a generalidade possível. Nada obriga n e p terem o mesmo quociente quando divididos por m. Então deve-se usar $n = km$ e $p = k'n$ no qual k pode ser diferente de k';

Definição 3.3. Dados $a, b, n \in \mathbb{Z}$, dizemos que a é congruente a b módulo n, denotado por

$$a \equiv b \pmod{n}$$

se n divide $a - b$. Isto é, existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Se $a \equiv b \pmod{n}$, dizemos também que a é equivalente a b módulo n.

Proposição 3.4. *Algumas propriedades básicas de congruências:*

(a) se $a \equiv b \pmod{n}$, *então* $a = b + kn$ *para algum* $k \in \mathbb{Z}$.

(b) para todo $a \in \mathbb{Z}$, *temos* $a \equiv a \pmod{0}$;

(c) para todo $a, b \in \mathbb{Z}$, *temos* $a \equiv b \pmod{1}$;

(d) se $a \equiv b \pmod{n}$, *então* $b \equiv a \pmod{n}$;

(e) se $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$, *então* $a \equiv c \pmod{n}$.

(f) $a \equiv b \pmod{n}$ *se e somente se a e b deixam o mesmo resto quando divididos por n;*

(g) se $a \equiv b \pmod{n}$, *então* $a + c \equiv b + c \pmod{n}$;

(h) se $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $a + c \equiv b + d \pmod{n}$;

(i) se $a \equiv b \pmod{n}$, *então* $ac \equiv bc \pmod{n}$;

(j) se $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $ac \equiv bd \pmod{n}$.

Demonstração. (a) Pela definição, se $a \equiv b \pmod{n}$, então $a - b = kn$ para algum $k \in \mathbb{Z}$. Logo, $a = b + kn$.

(b) Para todo $a \in \mathbb{Z}$, temos $a - a = k \cdot 0$, logo $a \equiv a \pmod{0}$.

(c) Para todo $a, b \in \mathbb{Z}$, existe $k \in \mathbb{Z}$ tal que $a - b = k \cdot 1$, logo $a \equiv b \pmod{1}$.

(d) Pela definição, se $a \equiv b \pmod{n}$, então $n|(a - b)$; isto é, $a - b = kn$ para algum $k \in \mathbb{Z}$. Então $b - a = (-k)n$ e $b \equiv a \pmod{n}$;

(e) Pela definição, se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, temos que existem $k, t \in \mathbb{Z}$ tais que $a - b = kn$ e $b - c = tn$. Somando as duas equações, temos $(a - b) + (b - c) = kn + tn$. Logo $a - c = (k + t)n$ e $a \equiv c \pmod{n}$. Esta prova poderia ser feita também utilizando a Proposição 3.3 (c): $n|(a - b)$ e $n|(b - c)$ e portanto $n|(a - b + b - c)$. Logo $n|(a - c)$ e $a \equiv c \pmod{n}$.

(f) ($\Longleftarrow$) Se a e b deixam o mesmo resto r quando divididos por n, então

$$\begin{aligned} a &= nq_a + r, \text{ e} \\ b &= nq_b + r. \end{aligned}$$

Logo, $a - b = n(q_a - q_b)$ e $a \equiv b \pmod{n}$.
($\Longrightarrow$) Se $a \equiv b \pmod{n}$, então $a - b = kn$ para algum $k \in \mathbb{Z}$. Suponha que

$$\begin{aligned} a &= nq_a + r_a, \text{ com } 0 \leq r_a < n, \text{ e} \\ b &= nq_b + r_b, \text{ com } 0 \leq r_b < n. \end{aligned}$$

Então $a - b = n(q_a - q_b) + (r_a - r_b)$. Como $a - b = kn$, temos

$$kn = n(q_a - q_b) + (r_a - r_b).$$

Logo, $n(k - q_a + q_b) = (r_a - r_b)$, isto é, $n|(r_a - r_b)$. Mas, $0 \leqslant |(r_a - r_b)| < n$. Portanto, $r_a - r_b = 0$ e $r_a = r_b$.
As demonstrações dos últimos quatro itens são deixadas a cargo do leitor. □

Definição 3.4. $p \in \mathbb{N}$ será chamado de primo se $p \neq 0$, $p \neq 1$ e os únicos números naturais divisores de p forem 1 e p.

Definição 3.5. Um número $n \in \mathbb{N}$ será chamado de *composto* se $n \neq 0$, $n \neq 1$ e n não for primo.

Proposição 3.5. *(Teorema Fundamental da Aritmética) Todo número $m \in \mathbb{N}$ maior ou igual a 2 é o produto de um ou mais primos e esta decomposição é única. Sendo p_i o i-ésimo menor primo, $m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ e não existe outra decomposição com primos e expoentes diferente desta.*

Demonstração. Faremos a prova da existência usando indução finita. O caso base é $m = 2$. Como 2 é primo, está trivialmente provado.

Suponha $m > 2$. Aplicaremos a HI para todos os números entre 2 e m. Isto é, para todo t, $2 \leqslant t \leqslant m$, temos $t = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}$. Usando a HI, provaremos que $m + 1$ pode ser decomposto como produto de primos. Se $m + 1$ é primo, a proposição está trivialmente provada. Se $m + 1$ não é primo, como ele é maior do que 2 e então é composto e pode ser escrito como $m + 1 = ab$. A HI pode ser aplicada a a e b, pois $a < m + 1$ e $b < m + 1$. Então a e b podem ser escritos como um produto de um ou mais primos. Logo, $m + 1$ também pode ser escrito da mesma forma.

Explicaremos formalmente este ponto. Assumiremos, sem perda de generalidade, que a e b são decompostos como

$$a = p_1^{e_1} p_2^{e_2} \dots p_f^{e_f} \text{ e } b = p_1^{h_1} p_2^{h_2} \dots p_f^{h_f} p_{f+1}^{h_{f+1}} \dots p_g^{h_g}$$

com $f \leqslant g$. Então

$$m + 1 = p_1^{e_1 + h_1} p_2^{e_2 + h_2} \dots p_f^{e_f + h_f} p_{f+1}^{h_{f+1}} \dots p_g^{h_g}$$

Isto é, $m+1$ pode ser decomposto como um produtos de primos também. Por exemplo, se $m+1 = 63000 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7$, então $m+1 = 420 \cdot 150 = (2^2 \cdot 3^1 \cdot 5^1 \cdot 7) \cdot (2 \cdot 3 \cdot 5^2)$

A prova da unicidade desta decomposição não será feita neste curso.

□

Exemplo 3.2.

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 9 &= 3^2 \\ 42 &= 2 \cdot 3 \cdot 7 \\ 126 &= 2 \cdot 3^2 \cdot 7 \\ 54 &= 2 \cdot 3^3 \\ 63000 &= 2^3 \cdot 3^2 \cdot 5^3 \cdot 7 \\ 300 &= 2^2 \cdot 3 \cdot 5^2 \\ 210 &= 2 \cdot 3 \cdot 5 \cdot 7 \end{aligned}$$

Dica: entre na página `http://www.wolframalpha.com` e digite um número na caixa de entrada. Será mostrado, entre outras coisas, os fatores primos do número. Experimente!

Dada uma fatoração de m em fatores primos, $m = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, os divisores de m são todos os números formados tomando-se cada expoente de p_i entre 0 e k_i e fazendo o produto entre eles. Por exemplo, encontraremos os divisores de $m = 2^2 3^3 5$. Os divisores são

$$2^0 3^0 5^0, 2^0 3^0 5^1, 2^0 3^1 5^0, 2^0 3^1 5^1, 2^0 3^2 5^0, 2^0 3^2 5^1, 2^0 3^3 5^0, 2^0 3^3 5^1, 2^1 3^0 5^0,$$
$$2^1 3^0 5^1, 2^1 3^1 5^0, 2^1 3^1 5^1, 2^1 3^2 5^0, 2^1 3^2 5^1, 2^1 3^3 5^0, 2^1 3^3 5^1, 2^2 3^0 5^0$$

Proposição 3.6. *(Euclides) O número de primos é infinito.*

Demonstração. Provaremos por contradição. Suponha que o número de primos seja finito; isto é, exista um conjunto finito $P = \{p_1, p_2, p_3, \cdots, p_n\}$ com todos os primos. Naturalmente, $p_1 = 2$, $p_2 = 3$, etc. Considere agora o número

$$m = (p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n) + 1$$

Se m é primo, ele é maior do que qualquer primo $p_i \in P$. Contradição, pois encontramos um primo que não pertence a P. Se m não é primo, existe um número primo q que divide m; isto é, $m = qk$. Se q for algum p_i, teremos que $q|(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n)$. Como $q|m$, $q|(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1)$, chegamos à conclusão de que $q|1$. Absurdo, pois q é primo e portanto maior do que 2.[1] De qualquer forma chegamos a uma contradição. Portanto o número de primos não pode ser finito. □

Definição 3.6. O máximo divisor comum (*greatest common divisor*, gcd), mdc, de dois inteiros n e m é o maior natural que divide ambos n e m. Definimos $\text{mdc}(0,0) = 0$.

[1] Sabemos que não é 2 porque o maior primo não é 2.

Exemplo 3.3.

$$\begin{aligned} \text{mdc}(24,10) &= \text{mdc}(2^3 \cdot 3, 2 \cdot 5) = 2 \\ \text{mdc}(126,54) &= \text{mdc}(2 \cdot 3^2 \cdot 7, 2 \cdot 3^3) = 2 \cdot 3^2 = 18 \\ \text{mdc}(33,15) &= \text{mdc}(3 \cdot 11, 3 \cdot 5) = 3 \end{aligned}$$

Dado $n \in \mathbb{Z}$, seja S_n o conjunto de todos os divisores positivos de n. Usando máx S para o máximo elemento do conjunto S, temos que, se $n \neq 0$ ou $m \neq 0$,

$$\text{mdc}(n,m) = \text{máx } S_n \cap S_m$$

Por exemplo,

$$\text{mdc}(24,10) = \text{máx } S_{24} \cap S_{10} = \text{máx } \{1,2,3,4,6,8,12,24\} \cap \{1,2,5,10\} = \text{máx } \{1,2\} = 2$$

Foi necessário colocar a condição que um dos números n ou m fosse diferente de 0 porque $S_0 = \mathbb{N}$. Então se esta definição fosse empregada para $\text{mdc}(0,0)$, teríamos $\text{mdc}(0,0) = S_0 \cap S_0 = \mathbb{N} \cap \mathbb{N} = \mathbb{N}$ e então a função máx não poderia ser aplicada.

Proposição 3.7. *Mostramos a seguir algumas propriedades da função mdc. Assumiremos que $n \neq 0$ ou $m \neq 0$.*

(a) se $d = mdc(n,m)$, então $d|n$ e $d|m$ (pela definição);

(b) se $d = mdc(n,m)$, então $d \leqslant |n|$ e $d \leqslant |m|$ pois todos os divisores de um número positivo são menores do que ele;

(c) $mdc(n,m) = mdc(m,n)$ pois $mdc(n,m) = máx\ S_n \cap S_m = máx\ S_m \cap S_n = mdc(m,n)$;

(d) $mdc(n,0) = |n|$. Se $n = 0$, $mdc(0,0) = 0 = |0|$. Se $n \neq 0$, todos os divisores de n são menores ou iguais a $|n|$. Portanto o maior deles é $|n|$. E qualquer número é divisor de 0:

$$mdc(n,0) = máx\ S_0 \cap S_n = máx\ \mathbb{N} \cap S_n = máx\ S_n = máx\ \{1, \ldots |n|\} = |n|$$

(e) $mdc(n,m) = mdc(|n|, |m|)$ pois se $d|n$ e $d|m$, então $d||n|$ e $d||m|$. Logo $S_n = S_{|n|}$ e $mdc(n,m) = S_n \cap S_m = S_{|n|} \cap S_{|m|} = mdc(|n|, |m|)$.

Proposição 3.8. *Dados $n, m \in \mathbb{Z}$ com $m \neq 0$, seja r o resto da divisão de n por m. Então $mdc(n,m) = mdc(m,r)$.*

Demonstração. Provaremos que todo divisor de n e m é também um divisor de m e r. Sendo $S_{n,m} = S_n \cap S_m$, provaremos que $S_{n,m} = S_{m,r}$.

Seja $b \in S_{n,m}$. Então $b|n$ e $b|m$. Temos que $n = qm + r$, $r = n - qm$. Pela Proposição 3.3 (c), como $b|n$ e $b|m$, então $b|r$. Como $b|r$ e $b|m$, temos $b \in S_{n,m}$, o que implica que $S_{n,m} \subset S_{m,r}$.

Seja $b \in S_{m,r}$. Então $b|m$ e $b|r$. Como $n = qm + r$, pela Proposição 3.3 (c) $b|n$ também. Temos que $b|n$ e $b|m$ e portanto $b \in S_{n,m}$ e $S_{m,r} \subset S_{n,m}$. Como $S_{n,m} \subset S_{m,r}$ e $S_{m,r} \subset S_{n,m}$, temos $S_{m,r} = S_{n,m}$.

□

Proposição 3.9. *Dada a sequência de inteiros $r_0, r_1, r_2, \ldots r_k, r_{k+1}$ na qual $r_0 = n$, $r_1 = m$ (com $n \geqslant m$), $n \neq 0$ e r_{i+1} é o resto da divisão de r_{i-1} por r_i para $i \geqslant 1$, então*

1. *existe um k tal que $r_k \neq 0$ e $r_{k+1} = 0$ e portanto temos uma sequência $r_0 \geqslant r_1 > r_2 > ... > r_k > r_{k+1} = 0$*

2. *$mdc(n, m) = r_k$;*

Demonstração. **Fato:** $r_0 \geqslant r_1 > r_2 > ... > r_k > r_{k+1}$
Prova do fato: provaremos por indução, suscintamente. $r_1 > r_2$ pois r_2 é o resto da divisão de r_0 por r_1. Assumindo, pela HI, que $r_{i-1} > r_i$, como r_{i+1} é o resto da divisão de r_{i-1} por r_i, temos que $0 \leqslant r_{i+1} < r_i$ e portanto $r_i > r_{i+1}$.
Fato: existe um k tal que $r_{k+1} = 0$. O conjunto composto pelos r_i´s é finito e portanto tem um menor elemento[2]. Se este elemento for $r_j \neq 0$, sempre podemos calcular r_{j+1} como o resto da divisão de r_{j-1} por r_j e portanto r_j não seria o menor elemento. Portanto algum elemento da sequência deve ser zero.

Provaremos agora que $\text{mdc}(n, m) = r_k$. Note que, para $i \geqslant 1$, $\text{mdc}(r_i, r_{i+1}) = \text{mdc}(r_{i+1}, r_{i+2})$ pela Proposição 3.8 e $\text{mdc}(r_k, 0) = r_k$ pela Proposição 3.7. Então

$$\text{mdc}(n, m) = \text{mdc}(r_0, r_1) = \text{mdc}(r_1, r_2) = \ldots \text{mdc}(r_k, r_{k+1}) = \text{mdc}(r_k, 0) = r_k$$

□

O algoritmo abaixo mostra como calcular o mdc de dois números. Este é o Algoritmo de Euclides e funciona mesmo que $a = b = 0$.

```
int mdc(int n, int m) {
   if ( n > m ) {
      a = n;
      b = m;
   }
   else {
      a = m;
      b = n;
   }
   while ( b != 0 ) {
      aux = b;
      b = a - b*(a/b); // resto da divisão de a por b
      a = aux;
   }
   return a;
}
```

[2]Por um teorema não apresentado neste texto, o Princípio da Boa Ordenação dos números naturais: todo conjunto não vazio de naturais possui um menor elemento.

Definição 3.7. Dois inteiros n e m são chamados de *primos entre si* se eles não têm divisor em comum além de 1; isto é, $mdc(n, m) = 1$.

Definição 3.8. O mínimo múltiplo comum (*least common multiple*, lcm) de dois números n e m tal que $n^2 + m^2 \neq 0$, denotado por mmc(n, m), é o menor natural diferente de 0 que é divisível por ambos n e m.

Exemplo 3.4. mmc$(6, 12) = 12$, pois 6 divide 12
mmc$(12, 7) = 12 \cdot 7 = 84$, pois 12 e 7 não tem fatores em comum
mmc$(10, 14) = 70$ (confira!)

O mdc e o mmc de dois números pode ser calculado utilizando o Teorema Fundamental da Aritmética. Sejam n e m inteiros com a seguinte decomposição em fatores primos:

$$\begin{aligned} n &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \dots p_l^{a_l} \\ m &= p_1^{b_1} p_2^{b_2} \dots p_k^{b_k} \end{aligned}$$

Assuminos, sem perda de generalidade, que $l \geqslant k$. O mdc de n e m é

$$p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \dots p_k^{\min\{a_k,b_k\}}$$

o mmc de n e m é

$$p_1^{\text{máx}\{a_1,b_1\}} p_2^{\text{máx}\{a_2,b_2\}} \dots p_k^{\text{máx}\{a_k,b_k\}} p_{k+1}^{a_{k+1}} \dots p_l^{a_l}$$

Não será feita a prova destas duas afirmações.

Conexão Computacional

Usando-se o operador `%` de Java/C/C++ pode-se obter o resto da divisão de dois números inteiros: `n%m` retorna o resto da divisão de `n` por `m`. A divisão `n/m` retorna o quociente de `n` por `m`, um inteiro.

Exercícios

3.1. Encontre o mmc e o mdc dos seguintes conjuntos de números.

(a) $100, 24$

(b) $14, 7, 24$

(c) $77, 28, 56, 42$

(d) $17, 29, 43, 71$

(e) $35, 25, 12$

3.2. Encontre a sequência $r_0, r_1, r_2, \ldots$ descrita na Proposição 3.9 considerando r_0, r_1 como

(a) $35, 24$

(b) $14, 130$

3.3. É possível que $n|mt$ mas n não divide m e n não divide t? Se sim, represente o exemplo que você encontrou com fatores primos e explique o que aconteceu.

3.4. Prove: todo número natural n composto tem um fator primo p tal que $p \leqslant \sqrt{n}$.

3.5. Prove novamente que o número de primos é infinito explicando cada passo do seu raciocínio.

3.6. Prove que, para $n, m \in \mathbb{N}$, $n^2 + m^2 \neq 0$, $\text{mmc}(n, m) \cdot \text{mdc}(n, m) = n \cdot m$.

3.7. Mostre que se dois números inteiros n e m são tais que $n = 6k_1 + 5$ e $m = 6k_2 + 5$, então nm pode ser escrito como $6k + 1$ para algum k inteiro.

3.8. Se $m|n$, $m|(n + m)$ e $m|n^2$? Se $m|n_i$ para $1 \leqslant i \leqslant k$, então

$$m| \sum_{i=1}^{k} n_i$$

?

3.9. 100! possui quantos zeros?

3.10. Cada item desta questão deve ser respondidado rapidamente. Considere que uma resposta foi satisfatória se foi feita em menos do que dois segundos (aproximadamente!).

(a) o número 17 está na tabuada?

(b) existe um primo que é a soma de dois números ímpares?

(c) é $2^{2^{100}} - 1$ par?

(d) se $\sqrt{n} \in \mathbb{N}$, n pode ser ímpar e primo? (☻)

(e) 37 é primo?

(f) a soma de dois primos pode ser um primo?

(g) é 7823694375 primo?

(h) qual número tem a tabuada que você considera mais difícil de memorizar?

(i) se n for par, $n^3 - n$ pode ser ímpar? (☻)

3.11. Substitua cada um dos símbolos # da seguinte expressão por `n` ou `m` de tal forma que ela seja verdadeira em Java (é uma expressão booleana). As três ocorrências de # podem ser substituídas por variáveis distintas. Assuma que `n` e `m` sejam inteiros.

```
# == (n/m)*# + (n%#)
```

Capítulo 4

Álgebra Booleana

A bibliografia indicada para este capítulo é Garnier [4].

Considere um conjunto B de elementos com

- pelo menos dois elementos distintos chamados de **identidades** e denotados por 0 e 1;
- duas operações binárias + e **.**, chamadas de **soma** e **produto**;
- uma operação unária chamada de **complemento**: $\overline{b}$ é o complemento de b;

Dizemos que B, junto com as suas operações, é uma **Álgebra Booleana** se os seguintes axiomas são satisfeitos, onde a, b e c são quaisquer elementos de B.

B_1 existência de identidades para + e **.**

$$\begin{array}{lrcl} \text{(a)} & a + 0 & = & 0 + a = a \\ \text{(b)} & a \,.\, 1 & = & 1 \,.\, a = a \end{array}$$

B_2 associatividade de + e **.**

$$\begin{array}{lrcl} \text{(a)} & (a + b) + c & = & a + (b + c) \\ \text{(b)} & (a \,.\, b) \,.\, c & = & a \,.\, (b \,.\, c) \end{array}$$

B_3 comutatividade de + e **.**

$$\begin{array}{lrcl} \text{(a)} & a + b & = & b + a \\ \text{(b)} & a \,.\, b & = & b \,.\, a \end{array}$$

B_4 distributividade de + sobre **.** e vice-versa

$$\begin{array}{lrcl} \text{(a)} & a + (b \,.\, c) & = & (a + b) \,.\, (a + c) \\ \text{(b)} & a \,.\, (b + c) & = & (a \,.\, b) + (a \,.\, c) \end{array}$$

B$_5$

(a) $a + \overline{a} = 1$
(b) $a \,.\, \overline{a} = 0$

Uma álgebra booleana com conjunto B, operações binárias + e **.**, operação unária **–** e símbolos 0 e 1 é denotada por $\langle B, +, \,.\,, -, 0, 1\rangle$.

Seja Γ_{AB} o conjunto de todas as fórmulas acima. Uma estrutura $\mathfrak{A} = \langle B, +, \,.\,, -, 0, 1\rangle$. é uma álgebra boolean se esta estrutura é modelo para Γ_{AB}. Isto é,

$$\mathfrak{A} \models \Gamma_{AB}$$

Então podemos encarar as fórmulas de Γ_{AB} de duas formas diferentes e equivalentes: a) elas são os axiomas da álgebra booleana e b) uma estrutura é uma álgebra booleana se é modelo para Γ_{AB}.

Alguns autores usam outros símbolos para +, **.** e **–**:

1. $\oplus$, $\star$, **-**
2. $\vee$, $\wedge$ e $\neg$
3. $+$, $\times$ e $-$

Usaremos +, **.** e **–**, mas lembre-se de que estes símbolos não têm o mesmo significado que na Aritmética. E 0 e 1 **não** são os números naturais 0 e 1. São apenas dois símbolos distintos.

Exemplos de Álgebras Booleanas

Exemplo 4.1. O cálculo proposicional com as operações $\vee$, $\wedge$ e $\neg$ formam uma álgebra booleana. Vejamos:

- $B = \{0, 1\}$, onde 0 e 1 são associados a F e V, respectivamente;
- +, **.** e **-** são associados a $\vee$, $\wedge$ e $\neg$, respectivamente

As tabelas para estas operações ficam assim:

a	b	$a + b$	$a \,.\, b$	$\overline{a}$
1	1	1	1	0
1	0	1	0	0
0	1	1	0	1
0	0	0	0	1

Para esta estrutura ser uma Álgebra Booleana, ela tem que ser modelo para as fórmulas de Γ_{AB}; isto é, as fórmulas deste conjunto têm que ser verdadeiras na estruturas. Verificaremos apenas algumas fórmulas, deixando as restantes como exercício.

- $a + 0 = a$. Pela tabela das operações dada acima, qualquer que seja o valor de a, o resultado de $a + 0$ é sempre a. Vejamos: a pode assumir apenas dois valores, 0 e 1. Então, pela tabela, $0 + 0 = 0$, $1 + 0 = 1$ e podemos concluir que $a + 0 = a$;

- $a + b = b + a$. Temos que conferir se esta fórmula é válida para todas as quatro combinações de valores para a e b. Isto é verdade quando a e b são ambos 0 ou ambos 1 e quando são diferentes, pois $1 + 0 = 0 + 1 = 1$.

Esta Álgebra Booleana é uma estrutura $\langle \{0, 1\}, \vee, \wedge, \neg, 0, 1 \rangle$.

Exemplo 4.2. Seja $S \neq \emptyset$ um conjunto e $\mathcal{P}(S)$ o conjunto dos subconjuntos de S (*power set*). Por exemplo, se $S = \{0, 1\}$,

$$\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$$

Seja $A \in \mathcal{P}(S)$. Então $\overline{A} = S - A$. Então $\langle \mathcal{P}(S), \cup, \cap, -, \emptyset, S \rangle$ é uma Álgebra Booleana.

Exercícios

4.1. Prove os itens abaixo. Considere que a e b são elementos de uma Álgebra Booleana.

(a) $\overline{\overline{a}} = a$

(b) $a + 1 = 1$

(c) $a \cdot 0 = 0$

(d) $(a + b) \cdot a = a$

4.2. Explique porque, em um mapa da Karnaugh, duas células adjacentes com número 1 trazem uma simplificação na fórmula final.

4.3. Simplifique os seguintes mapas de Karnaugh.

(a)

	x	$\overline{x}$
y	1	1
$\overline{y}$	0	0

(b)

	xy	$x\overline{y}$	$\overline{xy}$	$\overline{x}y$
z	1	0	1	0
$\overline{z}$	1	0	0	1

(c)

	xy	$x\overline{y}$	$\overline{xy}$	$\overline{x}y$
zt	1	1	1	0
$\overline{z}t$	0	0	1	1
$\overline{z}\overline{t}$	0	0	0	0
$z\overline{t}$	1	1	0	0

Capítulo 5

Teoria dos Conjuntos

5.1 Introdução

Há dois tipos de teoria dos conjuntos: a teoria ingênua e a teoria axiomática. Neste livro, veremos a teoria ingênua (*naïve set theory*) dos conjuntos, que admite alguns paradoxos como o paradoxo de Russel (veja abaixo). E apresentaremos a teoria axiomática, que não admite nenhum paradoxo.

O que é um conjunto? Na teoria ingênua dos conjuntos, um conjunto é uma coleção de elementos sem repetição. Esta coleção pode ser descrita enumerando-se os elementos ou fornecendo uma fórmula que todos os elementos devem obedecer. Por exemplo, os conjuntos

(a) $\{1, 5, 12, 334345\}$ e { Rollys-Royce, 23, azul, 'a', ♠, ✠} são descritos pela enumeração de elementos;

(b) $\{x : x \in \mathbb{N} \text{ e } x \text{ é par}\}$ e $\{x : x \in \mathbb{R} \text{ e } x^2 - x \leqslant 0\}$ são descritos por uma fórmula.

Freqüentemente utilizaremos uma Linguagem da Lógica de Primeira Ordem (LLPO) para descrever propriedades de conjuntos. A linguagem utilizada contém um único símbolo de constante, $\emptyset$ e um único símbolo de predicado binário, $\in$. Na descrição de conjuntos, outros símbolos são utilizados, como $\subset, \subseteq, \cap$, e $\cup$, mas estes podem ser definidos em termos de $\emptyset$ e $\in$.

Definição 5.1. Se um elemento x pertence a um certo conjunto A, dizemos $x \in A$. Se x não pertence a A, usamos $x \notin A$.

Definição 5.2. Usamos $A \subset B$ para A está contido em B; isto é, todos os elementos de A estão também em B. A é chamado de **subconjunto** de B.

Na LLPO, $A \subset B \longleftrightarrow \forall x\, (x \in A \longrightarrow x \in B)$. Note que $A \subset A$ para qualquer A.

Um símbolo em um conjunto pode significar duas coisas: o conjunto tem como elemento a) o símbolo ou b) o que significa o símbolo. Por exemplo, considere os conjuntos

$A = \{0, 1\}$
$B = \{A, 2, 3\}$

O conjunto B tem como elemento a letra A ou o conjunto $\{0, 1\}$? Usualmente o elemento é o que o símbolo significa. Então $B = \{\{0, 1\}, 2, 3\}$ e $\{0, 1\} \in B$. Se a letra A fosse o elemento de B, poderíamos afirmar que $\{0, 1\} \notin B$.

Exemplo 5.1. O paradoxo de Russel é o seguinte: suponha que exista um conjunto

$$C = \{x : x \notin x\}$$

Pergunta-se: $C \in C$? A resposta sim ou não resulta em uma contradição.[1] Então esta afirmação, $C \in C$ não pode ser verdadeira ou falsa.

Definição 5.3. Dois conjuntos A e B são iguais se eles têm os mesmos elementos. Usamos a notação $A = B$.

Na LLPO $A = B \longleftrightarrow (\forall x\ (x \in A \longleftrightarrow x \in B))$.
Para provar que dois conjuntos A e B são iguais, provamos $A \subset B$ e $B \subset A$.

Definição 5.4. Um subconjunto A de B tal que $A \neq B$ é chamado de subconjunto próprio de B.

Definição 5.5. Um conjunto que não contém elementos é chamado de conjunto vazio e indicado por $\emptyset$[2]. Então para todo x, $x \notin \emptyset$.

Proposição 5.1. *Propriedades do conjunto vazio.*

(a) *Para todo conjunto A, $\emptyset \subset A$. Prova: se $\emptyset \subset A$, então $x \in \emptyset$ implica em $x \in A$. Mas $x \in \emptyset$ é sempre falso. Temos uma implicação lógica do tipo $F \longrightarrow X$, onde X pode ser V ou F (depende se $x \in A$ ou não). Mas uma implicação do tipo $F \longrightarrow X$ é sempre verdadeira pela tabela verdade da implicação, $\longrightarrow$;*

(b) *O único subconjunto do conjunto vazio é o próprio conjunto vazio. Vejamos: $A \subset \emptyset$ implica em para todo $x \in A$, $x \in \emptyset$. Se $A \neq \emptyset$, teríamos $x \in \emptyset$, absurdo. Então não existe x tal que $x \in A$ e $A = \emptyset$.*

Alguns conjuntos de números são amplamente utilizados na Matemática:
$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, o conjuntos dos números naturais.
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$, o conjunto dos números inteiros.
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$, o conjunto dos números racionais, que podem ser expressos como a divisão de dois inteiros.
$\mathbb{R}$, o conjunto dos números reais, $\mathbb{R}^+ = \{x : x \in \mathbb{R} \text{ e } x \geqslant 0\}$, $\mathbb{R}^- = \{x : x \in \mathbb{R} \text{ e } x \leqslant 0\}$
$\mathbb{C}$, o conjunto dos números complexos.

Note que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

[1] Pense!

[2] O símbolo $\emptyset$ foi inspirado em uma letra do alfabeto Norueguês e Dinamarquês.

Denotamos por (a, b) o intervalo aberto dos números reais entre a e b:

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}$$

E por $[a, b]$ o intervalo fechado:

$$[a, b] = \{x \in \mathbb{R} : a \leqslant x \leqslant b\}$$

Os conjuntos $[a, b)$, $(a, b]$ são definidos similarmente. Assume-se em todos os casos, exceto em $[a, b]$, que $a \neq b$. E $[a, a] = \{a\}$.

Então $\mathbb{R}^+ = [0, \infty)$ e $\mathbb{R}^- = (-\infty, 0]$.

Definição 5.6. O conjunto das partes (*power set*) do conjunto A, denotado por $\mathcal{P}(A)$ ou 2^A, é composto por todos os subconjuntos de A. Então

$$\mathcal{P}(A) = 2^A = \{x : x \subset A\}$$

Ou seja, $x \in \mathcal{P}(A)$ sse $x \subset A$. Em notação lógica, $x \in \mathcal{P}(A) \longleftrightarrow x \subset A$.

Exemplo 5.2. Se $A = \{0, 1, 2\}$, $B = \{1\}$ e $C = \{\{1\}\}$, então

$$\begin{aligned}
&\mathcal{P}(A) = 2^A = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\} \\
&\mathcal{P}(B) = 2^B = \{\emptyset, \{1\}\} \\
&\mathcal{P}(C) = 2^C = \{\emptyset, \{\{1\}\}\} \\
&\mathcal{P}(\emptyset) = 2^\emptyset = \{\emptyset\}
\end{aligned}$$

O único subconjunto de $\emptyset$ é o próprio $\emptyset$. Então $x \in 2^\emptyset$ sse $x = \emptyset$.

Definição 5.7. Há algumas importantes operações entre conjuntos. Utilizaremos U para o conjunto contendo todos os elementos possíveis, o conjunto universo.

(a) união. A união de A com B, denotado por $A \cup B$, é definido como $\{x : x \in A \text{ ou } x \in B\}$. Como $A \cup (B \cup C) = (A \cup B) \cup C$ (veja os exercícios), os parênteses são desnecessários e podemos escrever simplesmente $A \cup B \cup C$;

(b) interseção. A interseção de A com B, denotado por $A \cap B$, é definido como $\{x : x \in A \text{ e } x \in B\}$. Como $A \cap (B \cap C) = (A \cap B) \cap C$, podemos escrever $A \cap B \cap C$;

(c) diferença. A diferença entre A e B, denotado por $A - B$, é o conjunto $\{x : x \in A \text{ e } x \notin B\}$;

(d) complemento em relação a U. O complemento do conjunto A, denotado por A^c, é definido como $U - A$;

(e) diferença simétrica entre conjuntos A e B, denotado por $A \triangle B$, é definido como $A \triangle B = (A - B) \cup (B - A)$.

(f) união dos conjuntos de um conjunto, denotado por $\bigcup S$, é definido como

$$\bigcup S = \{x : x \in A \text{ para algum } A \in S\}$$

Esta união é um conjunto que contém como elementos os elementos dos conjuntos de S.

Exemplo 5.3. Considere $A = \{0, 2, 4, 6\}, B = \{1, 3, 5\}, U = \mathbb{N}, C = \{0, 1, 3\}, R = \{\{0, 1\}, \{3\}, \{5, 7\}\}$ e $S = \{0, \{1, 5\}, \{\{\emptyset\}, 11\}, \emptyset\}$. Então:

- $A \cup B = \{0, 1, 2, 3, 4, 5, 6\}$
- $A \cap C = \{0\}$, $B \cap C = \{1, 3\}$
- $A - B = A$, $A - C = \{2, 4, 6\}$, $C - A = \{1, 3\}$, $R - A = R$
- $A \triangle B = \{0, 1, 2, 3, 4, 5, 6\}$, $A \triangle C = \{1, 2, 3, 4, 6\}$
- complemento em relação a U, $A^c = \{1, 3, 5, 7, 8, 9, 10, \ldots\}$
- $\bigcup R = \{0, 1, 3, 5, 7\}$, $\bigcup A = \bigcup B = \emptyset$
  Ou seja, $\bigcup R$ contém os elementos dos conjuntos $\{0, 1\}, \{3\}, \{5, 7\}$ que **pertencem** a R;
- $\bigcup S = \{1, 5, \{\emptyset\}, 11\}$ e $\bigcup(\bigcup S) = \{\emptyset\}$

Provaremos alguns fatos básicos sobre conjuntos.

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

Temos que provar que $(A \cup B) \cup C \subset A \cup (B \cup C)$ e $A \cup (B \cup C) \subset (A \cup B) \cup C$. Então

$$\begin{aligned} x \in (A \cup B) \cup C \quad & \text{sse} \quad x \in (A \cup B) \text{ ou } x \in C \\ & \text{sse} \quad (x \in A \text{ ou } x \in B) \text{ ou } x \in C \\ & \text{sse} \quad x \in A \text{ ou } (x \in B \text{ ou } x \in C) \\ & \text{sse} \quad x \in A \cup (B \cup C) \end{aligned}$$

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

Temos que provar que $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ e $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$.

$$\begin{aligned} x \in A \cup (B \cap C) \quad & \text{sse} \quad x \in A \text{ ou } x \in B \cap C \\ & \text{sse} \quad x \in A \text{ ou } (x \in B \text{ e } x \in C) \\ & \text{sse} \quad (x \in A \text{ ou } x \in B) \text{ e } (x \in A \text{ ou } x \in C) \\ & \text{sse} \quad (x \in A \cup B) \text{ e } (x \in A \cup C) \\ & \text{sse} \quad x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

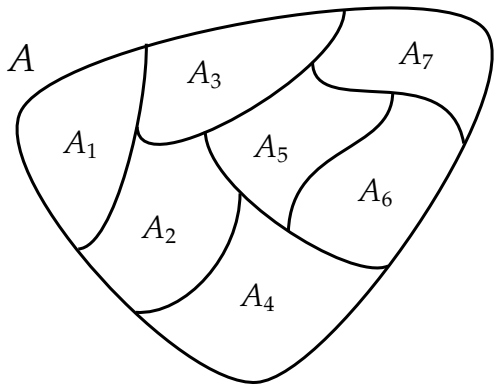


Figura 5.1: Partição de um conjunto A

Note que utilizamos alguns fatos do lógica para provar os fatos acima. Mais especificamente, utilizamos a associatividade do "ou" e a distributividade do "ou" sobre o "e". A saber,
$A \vee (B \vee C) \equiv (A \vee B) \vee C$
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
Usamos $\equiv$ para "logicamente equivalente".

Definição 5.8. Seja $A \neq \emptyset$ um conjunto. Uma **partição** de A é um conjunto P contendo subconjuntos de A tais que A é dado pela união dos subconjuntos de P e a interseção de dois destes subconjuntos é vazia. Ou seja,
$\bigcup P = A$ e para quaisquer $X, Y \in P$, $X \subset A$, $Y \subset A$, $X \cap Y = \emptyset$.

Exemplo 5.4. O conjunto $A = \{0, 1, 2, 3, 4\}$ pode ser particionado em conjuntos $\{0, 1\}$ e $\{2, 3, 4\}$. A partição P neste caso é $\{\{0, 1\}, \{2, 3, 4\}\}$.

Exemplo 5.5. O conjunto $P = \{(-\infty, 2], (2, 5), [5, \infty)\}$ é uma partição de $\mathbb{R}$. E não é uma partição de $\mathbb{N}$, pois $\bigcup P \neq \mathbb{N}$. Já $P = \{(-\infty, 2], [2, 5], [5, \infty)\}$ não é uma partição de $\mathbb{R}$ pois $(-\infty, 2] \cap [2, 5] = 2 \neq \emptyset$.

Exemplo 5.6. A Figura 5.1 mostra uma representação gráfica de uma partição de um conjunto A. Neste caso, $P = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7\}$. Qualquer elemento de A pertence a precisamente um dos conjuntos A_i. E

$$A = \bigcup_{i=1}^{7} A_i$$

Exemplo 5.7. O conjunto $\mathbb{N}$ pode ser particionado no conjunto dos pares e ímpares.

$$P = \{\{0, 2, 4, \ldots\}, \{1, 3, 5, \ldots\}\}$$

Exemplo 5.8. O conjunto

$$P = \{\mathbb{Z}, \ldots, (-2,-1), (-1,0), (0,1), (1,2), \ldots\} = \{\mathbb{Z}\} \cup \{(a, a+1) : a \in \mathbb{Z}\}$$

é uma partição de $\mathbb{R}$. Note que $\bigcup P = \mathbb{R}$ e se $A, B \in P$, $A \neq B$, então $A \cap B = \emptyset$.

Exercícios

5.1. Diga se os seguintes fatos são verdadeiros ou não. Justifique a sua afirmação.

(a) $2 \subset \{0, 1, 2\}$

(b) $\{0, 2\} \subset \{0, 1, 2\}$

(c) $\{0\} \in 2^{\{0,1,2\}}$

(d) $\{0, \emptyset\} \in 2^{\{0,1,2\}}$

(e) $2^A \subset 2^{2^A}$

(f) $P = \{\{0, 1\}, \{x : x \in \mathbb{N} \text{ e } x > 1\}\}$ é uma partição de $\mathbb{N}$

(g) $\bigcup\{0, \mathbb{N}, \pi\} = \mathbb{N}$

(h) $\bigcup 2^{\{0,1,2\}} = \{0, 1, 2\}$

(i) $\bigcup 2^{\mathbb{N}} = \mathbb{N}$

5.2. Diga se os seguintes fatos são verdadeiros ou não. Justifique a sua afirmação.

(a) $\emptyset \in \{\}$

(b) $\emptyset \subset \emptyset$

(c) $\emptyset \in \{\emptyset\}$

(d) $\emptyset \subset \{\emptyset\}$

(e) $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$

(f) $\emptyset \in 2^{\emptyset}$

5.3. Prove os seguintes fatos sobre conjuntos. Em cada um deles, deixe explícito as regras da lógica que você utilizou.

(a) $A \subset A$

(b) se $A \subset B$ e $B \subset C$, então $A \subset C$

(c) $A \cup A = A$ e $A \cap A = A$

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

(e) $(A^c)^c = A$

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

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

(h) se $A \subset B$, $A \cup B = B$ e $A \cap B = A$

(i) $((A - B) \cup (B - A)) \subset A \cup B$

5.4. Calcule $\mathcal{P}(A)$ para os seguintes conjuntos:

(a) $A = \{0, 1, 2, 3\}$

(b) $A = \emptyset$

(c) $A = \{\emptyset\}$

5.5. Cite três elementos do conjunto das partes de:

(a) $\mathbb{N}$

(b) $\mathbb{R}$

(c) $\{(a, b) : a, b \in \mathbb{N}\}$, o conjunto de todos os intervalos abertos.

5.6. Prove os seguintes fatos sobre o conjunto vazio:

(a) $2^\emptyset = \{\emptyset\}$

(b) $\emptyset \subset A$, para todo conjunto A. Explique detalhadamente as regras da lógica que você utilizou.

(c) $A \cup \emptyset = A$

(d) $A \cap \emptyset = \emptyset$

5.7. Paradoxo de Russel: considere $C = \{x : x \notin x\}$. Pergunta-se: $C \in C$? E $C \notin C$?

5.8. Encontre duas partições quaisquer para o conjunto $\{0, 1, 2, 3, 4, 5, 6\}$.

5.9. Encontre uma partição para o conjunto $\mathbb{R}^+$ com pelo menos três conjuntos.

5.10. Encontre uma partição para o conjunto $\mathbb{R}$ com infinitos conjuntos. Repita para $\mathbb{Q}$ e $\mathbb{N}$.

5.2 Diagramas de Venn

Um diagrama de Venn é uma representação gráfica de conjuntos e de relações entre eles. Um retângulo representa o conjunto **universo**, o conjunto que contém todos os possíveis elementos.[3] Conjuntos são representados por círculos ou retângulos dentro do universo. Se dois conjuntos A e B têm elementos em comum, os círculos que os representam se interceptam. Quando um diagrama de Venn é utilizado para representar uma operação entre conjuntos, como $A \cup B$, o resultado da operação é mostrado hachurado no diagrama.

Exercícios

5.11. Represente os seguintes conjuntos usando diagramas de Venn.

(a) $A \cap (B \cup C)$

(b) $A \subset B, B \subset C$

(c) $A \cap B \cap C$

(d) $A^c \cap B$

(e) $(A \cap B) \cup C$

(f) $(A \cup B)^c$

(g) $A^c \cap B^c$

(h) $(A - B) \cup (B - A)$

5.3 Relações

Relações permitem agrupar elementos de um ou mais conjuntos em um outro conjunto. Por exemplo, dado um conjunto de pessoas e um conjunto de idades destas pessoas, podemos construir uma relação nome×idade que relaciona a pessoa à sua idade. Um elemento desta relação poderia ser (João, 28) ou (Maria, 18) — iremos representar elementos de relações usando (e). Como um outro exemplo, dados os conjuntos de a) fabricantes de automóveis, b) nomes de automóveis, c) preços e d) potência do motor, podemos construir uma relação que relaciona todos estes itens. Dois elementos desta relação poderiam ser

(Honda, Fit, 46000, 76)
(Fiat, Pálio, 32000, 72)

Antes de definir relações, precisamos de algumas definições.

[3] Este é o único lugar onde utilizaremos o conjunto Universo. Este conjunto dá origem a um paradoxo.

Definição 5.9. Um **par ordenado** é uma lista ordenada de dois elementos que é representado da forma (a, b). A ordem dos elementos é importante: $(a, b) \neq (b, a)$ e $(a, b) = (c, d)$ se e somente se $a = c$ e $b = d$.

Exemplo 5.9. Utilizando o conjunto $\mathbb{N}$, temos os pares ordenados $(1, 2)$, $(7, 3)$ e $(1024, 10)$.

Definição 5.10. Uma **n-tupla** é uma lista ordenada $(a_1, a_2, \ldots a_n)$ de elementos. A ordem dos elementos é importante. E

$$(a_1, a_2, \ldots a_n) = (b_1, b_2, \ldots b_n)$$

se e somente se $a_i = b_i$ para $1 \leqslant i \leqslant n$.

Definição 5.11. Um par ordenado pode ser representado utilizando conjuntos: $(a, b) =_{def} \{\{a\}, \{a, b\}\}$. E uma n-tupla $(a_1, a_2, \ldots a_n)$ é definida como $((a_1, a_2, \ldots a_{n-1}), a_n)$ para $n \geqslant 3$.

Definição 5.12. O **produto cartesiano** entre dois conjuntos A e B, denotado por $A \times B$, é o conjunto de todos os pares ordenados onde o primeiro elemento pertence a A e o segundo a B. Ou seja

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

No caso geral, o produto cartesiano dos conjuntos A_1, A_2, ..., A_n é definido como

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

$A_1 \times A_2 \times \ldots \times A_n$ pode ser denotado por $\prod_{i=1}^{n} A_i$. No caso geral, o índice pode ser um conjunto qualquer:

$$\prod_{i \in I} A_i$$

Exemplo 5.10. Alguns exemplos de produto cartesiano.

1. se $A = \{0, 2, 4\}$ e $B = \{1, 3\}$, então

$$A \times B = \{(0, 1), (0, 3), (2, 1), (2, 3), (4, 1), (4, 3)\}$$

2. $\mathbb{N}^2 = \{(a, b) : a, b \in \mathbb{N}\}$

3. $\mathbb{R}^2$ é o conjuntos dos pares de números reais, o plano cartesiano.

4. $\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) : a \in \mathbb{Z} \text{ e } b \in \mathbb{Z}^*\}$.

5. o produto cartesiano $\emptyset \times A$ é o conjunto vazio.

Definição 5.13. Qualquer subconjunto de $A \times B$ é chamado de **relação** entre A e B. No caso geral, qualquer subconjunto de $A_1 \times A_2 \times \ldots \times A_n$ é uma relação n-ária entre os conjuntos A_i.

Note que na definição acima, n pode ser 1. Então qualquer subconjunto B de um conjunto A é uma relação **unária** em A.

Exemplo 5.11. São exemplos de relações:

1. se $A = \{0, 2, 4\}$ e $B = \{1, 3\}$, então $R = \{(0, 3), (4, 1)\}$ e $S = \{(2, 1), (4, 1), (2, 3)\}$ são relações em A e B;
2. O conjunto dos números naturais pares é uma relação unária em $\mathbb{N}$.
3. o conjunto de todos os pares de números naturais onde o primeiro é divisível pelo segundo,

   $$\{(0, 1), (0, 2), \ldots, (2, 1), (2, 2), \ldots, (3, 1), (3, 3), (4, 1), (4, 2), (4, 4), \ldots\}$$

   Esta é uma relação em $\mathbb{N}^2$. Ou em $\mathbb{R}^2$, se preferir;
4. o conjunto dos pontos (x, y) em $\mathbb{R}^2$ tal que $x^2 + y^2 = 1$;
5. o conjunto dos pares (a, b) tal que $a, b \in \mathbb{N}$ e a divide b;
6. o conjunto dos pares (a, b) em $\mathbb{R}$ tal que a é menor do que b.

Definição 5.14. Usamos a notação $a\ R\ b$ sempre que R é uma relação binária e $(a, b) \in R$.

Exemplo 5.12. A relação $<$ sobre $\mathbb{R}$ é normalmente utilizada na forma $a < b$ e não como $(a, b) \in <$. Contudo, pode-se usar esta última forma.

Definição 5.15. Seja $R \subset A \times B$. Então

(a) $Dom(R) = \{a \in A : \exists b \in B \text{ e } a\ R\ b\}$. O conjunto $Dom(R)$ é o domínio (*domain*) de R;

(b) $Im(R) = \{b \in B : \exists a \in A \text{ e } a\ R\ b\}$. O conjunto $Im(R)$ é a imagem (*image*) de R.

Definição 5.16. Se $R \subset A \times B$, a relação inversa R^{-1} é definida como
$R^{-1} = \{(b, a) : (a, b) \in R\}$
Claramente, $Dom(R) = Im(R^{-1})$, $Im(R) = Dom(R^{-1})$.

Exemplo 5.13. se $A = \{0, 2, 4\}$, $B = \{1, 3\}$ e $R = \{(0, 3), (4, 1)\}$, então $R^{-1} = \{(3, 0), (1, 4)\}$.

Exemplo 5.14. A Figura 5.5 representa o grafo não dirigido $G = (V, E)$ no qual $V = \{0, 1, 2, 3, 4\}$ e

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

Uma relação binária $R \subset A \times B$ é usualmente representada por duas elipses, uma para A e outra para B, por pontos em A e B para os elementos destes conjuntos e setas ligando um elemento $a \in A$ a $b \in B$ sempre que (a, b) pertence à relação.

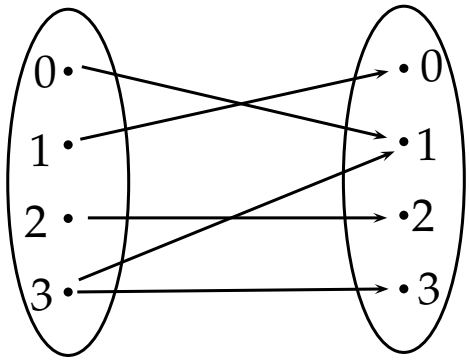


Figura 5.2: Representação de uma relação graficamente

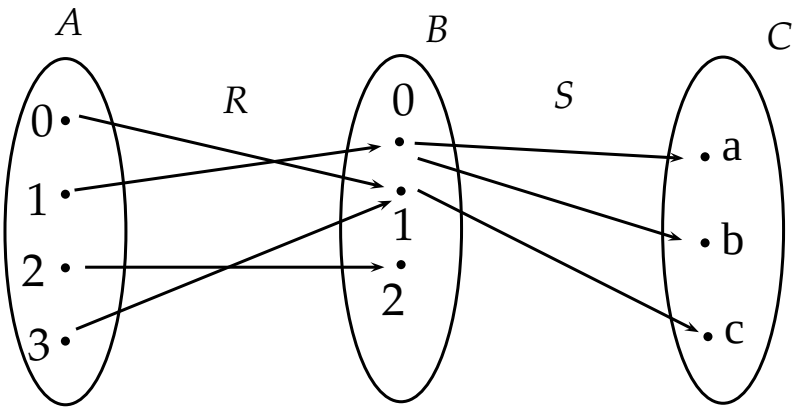


Figura 5.3: Representação da composição de duas relações

Exemplo 5.15. A Figura 5.2 representa graficamente a seguinte relação sobre $\{0, 1, 2, 3\}$:

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

Definição 5.17. Se $R \subset A \times B$ e $S \subset B \times C$, então a relação composta $R \circ S \subset A \times C$ é definida como

$$R \circ S = \{(a, c) : \text{ existe } b \in B \text{ tal que } (a, b) \in R \text{ e } (b, c) \in S\}$$

Exemplo 5.16. Dados os conjuntos $A = \{0, 1, 2, 3\}$, $B = \{0, 1, 2\}$, e $C = \{a, b, c\}$ e as relações $R \subset A \times B$, $S \subset B \times C$ definidas como

$$R = \{(0, 1), (1, 0), (2, 2), (3, 1)\}$$
$$S = \{(0, a), (0, b), (1, c)\}$$

A relação composta $R \circ S = \{(0, c), (1, a), (1, b), (3, c)\}$ pode ser claramente vista pela Figura 5.3. O par (x, y) pertence à $R \circ S$ se, partindo-se de $x \in A$ e seguindo-se as setas, é possível chegar em $y \in C$.

Proposição 5.2. *Apresentamos abaixo algumas propriedades de relações.*

1. $R \circ (S \circ T) = (R \circ S) \circ T$
2. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
3. $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$

As provas destes fatos são deixadas como exercícios.

Uma relação binária $R \subset A \times B$ pode ser representada por uma matriz M com $|A|$ linhas e $|B|$ colunas, no qual $|A|$ é o número de elementos do conjunto A. Cada linha da matriz M representa um elemento de A e cada coluna, um elemento de B. Se $a \in A$ é o elemento correspondente à linha i e $b \in B$ o elemento correspondente à linha j, então

$$M_{ij} = \begin{cases} 1 & \text{se } (a, b) \in R \\ 0 & \text{caso contrário} \end{cases}$$

Exemplo 5.17. Se $A = \{0, 2, 4\}$, $B = \{1, 3, 5, 7\}$ e $R = \{(0, 3), (2, 1), (2, 5), (4, 1), (4, 7)\}$, a matriz que representa é

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Se V é um conjunto finito, uma relação binária $E \subset V \times V$ pode ser representada por um grafo dirigido G e vice-versa. Há um vértice x no grafo para cada elemento $x \in V$. Há uma seta de x para y se e somente se $x \, E \, y$. Se $x \, E \, y$ implicar $y \, E \, x$, então as setas são substituídas por linhas entre os vértices.

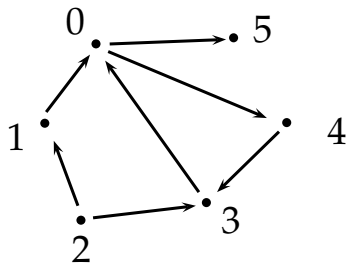


Figura 5.4: Exemplo de um grafo que corresponde a uma relação

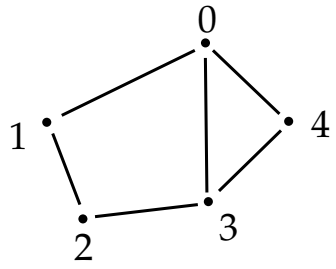


Figura 5.5: Exemplo de um grafo não dirigido

Exemplo 5.18. Se $V = \{0, 1, 2, 3, 4, 5\}$ e $E = \{(0, 4), (0, 5), (1, 0), (2, 1), (2, 3), (3, 0), (4, 3)\}$, o grafo que representa esta relação está na Figura 5.4.

Exercícios

5.12. Represente $(0, 1)$ e a 3-tupla $(2, 5, 3)$ como conjuntos de acordo com a definição de par ordenado e 3-tupla.

5.13. Prove os seguintes fatos sobre relações:

(a) $A \times B = \emptyset$ se e somente se $A = \emptyset$ ou $B = \emptyset$.

(b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

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

(d) $B \subset C$ implica em $A \times B \subset A \times C$

(e) $A \times B \neq B \times A$

5.14. Se $R \subset A \times B$ e $x \in R$, então temos que $R \subset A \times B \subset Y$ para algum Y. Calcule Y em função de A e B.

5.15. Sejam $R \subset A \times B$ e $S \subset B \times C$. Todos os conjuntos são finitos e as matrizes que representam as relações são M_R e M_S. Prove que $M_R M_S$ é a matriz que representa a relação composta $R \circ S$.

5.16. Prove os fatos da Proposição 5.2.

5.17. Prove que $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ se e somente se $a = c$ e $b = d$.

5.18. Prove que $Dom(R) = Im(R^{-1})$ e $Im(R) = Dom(R^{-1})$ (trivial).

5.19. Defina explicitamente a relação R que é o conjunto de todos os círculos concêntricos com centro em $(0, 0)$. R é subconjunto de qual conjunto?

5.20. Sejam $A = \{0, 2, 4\}$, $B = \{1, 3, 5\}$, $R \subset A \times B$, $R = \{(0, 1), (0, 5), (2, 3), (4, 3), (4, 5)\}$, $S \subset B^2$, $S = \{(1, 1), (3, 1), (5, 1), (3, 5)\}$. Baseado nestes conjuntos, faça:

(a) a representação gráfica de R;

(b) a representação em forma de matriz de R e S;

(c) a relação composta $R \circ S$;

(d) R^{-1};

(e) $S \circ S$;

(f) a representação em forma de matriz de $S \circ S$;

(g) a representação em forma grafos de S;

(h) o domínio e a imagem de R e S.

5.4 Funções

Uma **função** $f : A \longrightarrow B$ é uma relação $f \subset A \times B$ tal que:

(a) $Dom(f) = A$;

(b) para todo x, y e z, se $(x, y) \in f$ e $(x, z) \in f$ então $y = z$.

Na linguagem da lógica de primeira ordem,

$$(x, y) \in f \wedge (x, z) \in f \longrightarrow y = z$$

ou

$$\forall x \forall y \forall z \, ((x, y) \in f \wedge (x, z) \in f \longrightarrow y = z)$$

O único b tal que $(a, b) \in f$ é denotado por $f(a)$ ou, em algumas ocasiões, fa. Escreve-se $f(x)$ para denotar: a) uma função f que toma um único parâmetro e b) o valor y tal que $y = f(x)$. O significado utilizado, a) ou b), pode ser deduzido do contexto.

Definição 5.18. Dada uma função $f : A \longrightarrow B$, o conjunto A é chamado de **domínio** de f (*domain*) e B chamado de **contra-domínio** de f (*codomain*). O conjunto $\{b : \exists a\ (a \in A \wedge f(a) = b)\}$ é a **imagem** (*range, image*) de f. O domínio, contra-domínio e imagem de f são denotados por $Dom(f)$, $Codom(f)$ e $Im(f)$, respectivamente.

Exemplo 5.19. A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = e^x$ tem domínio $\mathbb{R}$, contra-domínio $\mathbb{R}$ e imagem $\mathbb{R}_*^+$.

Exemplo 5.20. A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $f(x) = x^2 - 4x + 3$ tem domínio $\mathbb{R}$, contra-domínio $\mathbb{R}$ e imagem $[-1, \infty)$.

O conjunto A pode ser qualquer conjunto, inclusive um produto cartesiano:
$f : A^n \longrightarrow B$ Neste caso, se $(a_1, a_2, \ldots, a_n, b) \in f$ usamos a notação $b = f(a_1, a_2, \ldots, a_n)$. Da mesma forma, B também pode ser um produto cartesiano: $f : A^n \longrightarrow B^m$ Neste caso, se $(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m) \in f$ usamos a notação $(b_1, b_2, \ldots, b_m) = f(a_1, a_2, \ldots, a_n)$.

Exemplo 5.21. Um autômato finito M é uma 5-tupla $(Q, \Sigma, \delta, q_0, F)$ no qual Q é um conjunto finito de estados, Σ é um conjunto finito de símbolos, δ é uma função $\delta : Q \times \Sigma \longrightarrow Q$, $q_0 \in Q$ e $F \subset Q$. Um exemplo de autômato é $M = (\{q_0, q_1\}, \{0, 1\}, \delta, q_0, \{q_1\})$ no qual δ é definida como:

δ	0	1
q_0	q_0	q_1
q_1	q_1	q_0

Isto é, por exemplo, $\delta(q_0, 1) = q_1$.

Exemplo 5.22. Uma máquina de Turing M é uma quádrupla (Q, Σ, I, q) na qual Q e Σ são conjuntos finitos de estados e de símbolos, I é um conjunto de instruções, $I \subset Q \times \Sigma \times Q \times \Sigma \times D$, $D = \{-1, 0, 1\}$ e $q \in Q$ é chamado de estado inicial. Como exemplo temos $M = (\{q_0, q_1, q_s, q_n\}, \{0, 1, \square\}, I, q_0)$ tal que

$$I = \{(q_0, 0, q_0, 0, 1), (q_0, \square, q_s, \square, 0), (q_0, 1, q_n, 1, 0)\}$$

Definição 5.19. Dado $f : A \longrightarrow B$, $f(X) = \{f(x) : x \in X\}$. Naturalmente, $f(\emptyset) = \emptyset$.

Como exemplo, para $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$, $X = (0, 3)$, $f(X) = (0, 9)$.

Definição 5.20. Uma função $f : A \longrightarrow B$ é chamada de **injetora** (*injective*) se para quaisquer $x, y \in A$, $f(x) = f(y)$ implica em $x = y$.

Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ é injetora se qualquer reta horizontal ($y = k$) cruza com o gráfico de f em no máximo um ponto.

Definição 5.21. Uma função $f : A \longrightarrow B$ é chamada de **sobrejetora** (*onto, surjective*) se $Im(f) = B$.

Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ é sobrejetora se qualquer reta horizontal ($y = k$) cruza com o gráfico de f em pelo menos um ponto.

Definição 5.22. Uma função $f : A \longrightarrow B$ é chamada de **bijetora** (*one-to-one, bijective*) se ela é injetora e sobrejetora.

Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ é bijetora se qualquer reta horizontal ($y = k$) cruza com o gráfico de f em exatamente um ponto.

Definição 5.23. A função identidade no conjunto A, $I_A : A \longrightarrow A$ é definida como $I_A(x) = x$. Em geral, deixa-se implícito o conjunto A, usando-se I para qualquer função identidade.

Definição 5.24. Dadas as funções $f : A \longrightarrow B$ e $g : B \longrightarrow C$, a composição de f com g é definida analogamente à definição de composição de relações. Isto é, a composição de f com g, denotada por $g \circ f$ é definida como

$$g \circ f : A \longrightarrow C \text{ tal que } (g \circ f)(x) = g(f(x))$$

Definição 5.25. Inversas de funções são definidas analogamente a inversas de relações. Mas exige-se que a função seja bijetora. Então, dada uma função bijetora $f : A \longrightarrow B$, a função inversa de f, denotada por f^{-1} é definida como

$$f^{-1}(y) = x \text{ sse } f(x) = y$$

Naturalmente, $f^{-1} : B \longrightarrow A$.

Proposição 5.3. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstração. Provaremos que, para todo z, $(g \circ f)^{-1}(z) = f^{-1}(g^{-1}(z))$.

$$\begin{aligned}
& (g \circ f)^{-1}(z) = x \\
\text{sse} \quad & (g \circ f)(x) = z \\
\text{sse} \quad & g(f(x)) = z \\
\text{sse} \quad & \text{existe } y = f(x) \text{ e } g(y) = z \\
\text{sse} \quad & x = f^{-1}(y) \text{ e } y = g^{-1}(z) \\
\text{sse} \quad & x = f^{-1}(g^{-1}(z)) \\
\text{sse} \quad & x = f^{-1} \circ g^{-1}(z)
\end{aligned}$$

□

A partir de qualquer função injetora pode-se construir uma função bijetora e portanto invertível. Por exemplo,

$$f : [0, 1] \longrightarrow \mathbb{R} \text{ tal que } f(x) = x^2$$

não é sobrejetora (e portanto não é bijetora e não tem inversa). Mas como $f([0, 1]) = [0, 1]$, podemos restringir o codomínio para torná-la sobrejetora:

$$g : [0, 1] \longrightarrow [0, 1], g(x) = f(x)$$

g é bijetora. Então dada uma função $f : A \longrightarrow B$ injetora qualquer, $g : A \longrightarrow f(A)$ tal que $g(x) = f(x)$ para todo $x \in A$ é bijetora.

Freqüentemente é necessário utilizar diversos conjuntos que são diferenciados por um índice. O exemplo clássico é de um vetor: usamos v_i para o i-ésimo elemento de v. Ou M_{ij} para o elemento da linha i e coluna j da matriz M. Ou M_i para a linha i da matriz, um outro conjunto indexado, um vetor. Este uso de índices com conjuntos é definido formalmente a seguir.

Definição 5.26. Uma **família de elementos** $F = \{A_\alpha : \alpha \in \Gamma\}$ é definida como uma função $f : \Gamma \longrightarrow A$ tal que $A_\alpha = f(\alpha)$. A família F pode ser denotada por $(A_\alpha)_{\alpha\in\Gamma}$ ou $\{A_\alpha\}_{\alpha\in\Gamma}$.

Se os elementos A_α são conjuntos, temos uma **família de conjuntos** indexados por um índice. Neste caso, A contém todos os conjuntos A_α.

Exemplo 5.23. O conjunto dos pares A_0 e o conjunto dos ímpares A_1 podem ser colocados em uma família $F = (A_i)_{i\in\{0,1\}}$.

Exemplo 5.24. Um vetor $v = (v_1, v_2, \ldots v_n)$ no qual $v_i \in A$ é uma família de elementos

$$f : \{1, 2, \ldots n\} \longrightarrow A$$

tal que $f(i) = v_i$. Também podemos denotar esta família por $(v_i)_{1\leqslant i\leqslant n}$.

Exemplo 5.25. Os intervalos abertos $(n, n+1)$ tal que $n \in \mathbb{N}$ podem ser colocados em uma família tal que $A_n = (n, n+1)$. A família é a função

$$f : \mathbb{N} \longrightarrow \mathbb{R}$$

tal que $f(i) = (i, i+1)$. Note que

$$\bigcup_{i\in\mathbb{N}} A_i = \mathbb{R}^* - \mathbb{N}$$

Exemplo 5.26. Uma seqüência $a_0, a_1, a_2, \ldots$ é uma família indexada por $\mathbb{N}$, denotada por $\{a_i\}_{i\in\mathbb{N}}$. Vejamos um exemplo:

$$1, \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots$$

Esta família é a função $f : \mathbb{N} \longrightarrow \mathbb{R}$ tal que $f(i) = \frac{1}{2^i}$. Podemos escrever

$$\sum_{i\in\mathbb{N}} a_i = 2$$

Definição 5.27. Dada uma função $f : A^n \longrightarrow A$ e um conjunto $B \subset A$, dizemos que B é fechado sobre a operação f quando sempre que $a_i \in B$ para $1 \leqslant i \leqslant n$, temos $f(a_1, a_2, \ldots a_n) \in B$.

Exemplo 5.27. Sendo P o conjunto dos números inteiros pares, $P \subset \mathbb{Z}$, temos que a soma dos inteiros é fechada sobre P. Dados dois pares, a soma deles é par. Isto é, dados $n, m \in P$, $n + m \in P$. Sendo I o conjunto dos inteiros ímpares, I não é fechado sobre a operação soma pois a soma de dois ímpares é par, que não pertence a I. Isto é, dados $n, m \in I$, $n + m \in P$.

Exemplo 5.28. Seja M o conjunto de todas as matrizes reais $n \times n$ para qualquer n e $T \subset M$ o conjunto de todas as matrizes invertíveis (para $A \in T$, existe A^{-1} tal que $A \cdot A^{-1} = A^{-1} \cdot A = I$, no qual I é a matriz identidade). Então T é fechado sobre a operação de multiplicação de matrizes, denotada por $(\cdot)$. Dadas duas matrizes $A, B \in T$, $A \cdot B \in T$: como $A, B \in T$, existem A^{-1} e B^{-1} inversas de A e B. E a inversa de $A \cdot B$ é $B^{-1} \cdot A^{-1}$. Ou seja, o produto de duas matrizes invertíveis é invertível também.

Exercícios

5.21. Classifique as funções abaixo como injetoras, sobrejetoras, bijetoras ou nenhuma destas opções.

(a) $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = x^2 - x + 1$;

(b) $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = 2^x$;

(c) $f : \mathbb{R} \longrightarrow \mathbb{R}^+ - \{0\}$ tal que $f(x) = 2^x$;

(d) $f : \mathbb{R} \longrightarrow \mathbb{N}$ tal que $f(x) = \lfloor x \rfloor$;

5.22. Sejam A e B dois conjuntos finitos cujos tamanhos são n e m. Pergunta-se:

(a) quantas funções diferentes de A em B existem?

(b) quantas funções diferentes e injetoras de A em B existem?

(c) quantas funções diferentes e sobrejetoras de A em B existem? (**difícil!**)

5.23. Prove que se f é invertível, f^{-1} é invertível e $(f^{-1})^{-1} = f$.

5.24. Dadas funções f e g de $\mathbb{R}$ em $\mathbb{R}$ tal que $f(x) = x^2 + 1$ e $g(x) = x^3 - 1$, encontre $f \circ g$ e $g \circ f$.

5.25. Dada $f : \mathbb{R} - \{1\} \longrightarrow \mathbb{R} - \{-1\}$ tal que $f(x) = \frac{x}{1-x}$, encontre a sua inversa. Confira que $f \circ f^{-1} = f^{-1} \circ f = x$.

5.26. Quais das relações abaixo são funções? E para as que são, qual o domínio, contra-domínio e imagem?

(a) $\{(a, b) : a, b \in \mathbb{R} \text{ e } a^2 + b = 1\}$

(b) $\{(a, b) : a, b \in \mathbb{R}^+ \text{ e } a^2 + b^2 = 1\}$

(c) $\{(a, b) : a, b \in \mathbb{R} \text{ e } a + b^2 = 1\}$

(d) $\{(a, b) : a, b \in \mathbb{N} \text{ e } a = b\}$

5.27. Mostre como uma matriz pode ser vista como uma família de conjuntos.

5.28. Seja A_α o conjunto de todos os divisores de $\alpha \in \mathbb{N}$. Se $P = \bigcup_{\alpha\in\mathbb{N}}\{A_\alpha\}$, calcule o conjunto $\bigcup P$. Justifique cada passo da sua resposta.

5.29. Prove os itens abaixo. Considere que A_α é uma família indexada de conjuntos com $\alpha \in I$.

(a) se $A \subset B$, então $f(A) \subset f(B)$;

(b) se $A \subset B$, então $f^{-1}(A) \subset f^{-1}(B)$;

(c) $f(\bigcup_{\alpha\in I} A_\alpha) = \bigcup_{\alpha\in I} f(A_\alpha)$

(d) $f(\bigcap_{\alpha\in I} A_\alpha) \subset \bigcap_{\alpha\in I} f(A_\alpha)$

(e) $\bigcup_{\alpha\in I}(X - A_\alpha) = X - \bigcap_{\alpha\in I} A_\alpha$

(f) $\bigcap_{\alpha\in I}(X - A_\alpha) = X - \bigcup_{\alpha\in I} A_\alpha$

5.30. Considere uma família de conjuntos $F = \{A_\alpha : \alpha \in \mathbb{R}\}$ tal que $A_\alpha = \{d : d \text{ é dígito de } \alpha\}$. Por exemplo, $A_n = \{n\}$ para todo $n \in \mathbb{N}, 0 \leqslant n \leqslant 9$, $A_{3.1415} = \{1, 3, 4, 5\}$, $A_{769} = \{6, 7, 9\}$. Calcule

$$\bigcup_{\alpha\in\mathbb{R}} F$$

5.31. Responda se as seguintes operações são fechadas ou não. Justifique.

(a) operação de divisão sobre $\mathbb{N} \subset \mathbb{Q}$ (isto é, estamos usando a divisão em $\mathbb{Q}$. Idem para os outros itens);

(b) multiplicação sobre $\mathbb{N} \subset \mathbb{R}$;

(c) subtração sobre $\mathbb{N} \subset \mathbb{Z}$;

(d) $\sqrt{n}$ sobre $\mathbb{N} \subset \mathbb{R}$;

(e) composição de funções sobre $B \subset A$ no qual A é o conjunto de todas as funções de $\mathbb{N}$ em $\mathbb{N}$ e B é o subconjunto de A que contém apenas funções bijetoras.

5.32. Um autômato finito não determinístico é definido como uma 5-tupla $(Q, \Sigma, \delta, q_0, F)$ sendo que a função δ é tal que

(a) $\delta(q, \epsilon)$ é permitido, no qual ϵ é a cadeia vazia de símbolos, $\epsilon \notin \Sigma$;

(b) o resultado de $\delta(q, s)$ é um subconjunto de Q

Baseado nestas informações, defina o domínio e contra-domínio de δ.

5.5 Funções Especiais

Nesta seção apresentaremos algumas funções especiais.

$\lceil . \rceil : \mathbb{R} \longrightarrow \mathbb{Z}$ tal que $\lceil x \rceil$ é o menor inteiro maior ou igual a x. Em termos de conjuntos,

$$\lceil x \rceil = \min\{n : n \in \mathbb{Z} \text{ e } n \geqslant x\}$$

$\lfloor . \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ tal que $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x. Em termos de conjuntos,

$$\lfloor x \rfloor = \text{máx } \{n : n \in \mathbb{Z} \text{ e } n \leqslant x\}$$

Por exemplo, $\lceil 2.3 \rceil = 3$, $\lceil 3.7 \rceil = 4$ e $\lceil -5.4 \rceil = -5$. E $\lfloor 2.3 \rfloor = 2$, $\lfloor 3.7 \rfloor = 3$ e $\lfloor -5.4 \rfloor = -6$. Algumas propriedades importantes destas funções são dadas abaixo:

- a representação de um número inteiro k na base b ocupa $\lfloor \log_b k \rfloor + 1$ dígitos. Então para representar um inteiro k em binário precisamos de $\lfloor \log_2 k \rfloor + 1$ bits;
- $\lfloor x \rfloor \leqslant x \leqslant \lfloor x \rfloor + 1$;
- $x \leqslant \lceil x \rceil \leqslant x + 1$;
- a expressão $\lfloor x + 0,5 \rfloor$ arredonda x para o inteiro mais próximo;
- $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$ para todo $k \in \mathbb{N}$.

Em computabilidade se usa o conceito de *função parcial*.

Definição 5.28. Uma função parcial é uma função que pode não estar definida para todos os elementos do domínio.

Por exemplo, $f : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $f(x) = 1/x$ é uma função parcial pois $f(0)$ não está definida. Um programa de computador[4] pode implementar uma função $f : \mathbb{N} \longrightarrow \mathbb{N}$ pois as entradas e saídas são representadas em binário e portando podem ser consideradas números inteiros. Contudo, para algumas entradas certo programa pode não parar. A função que este programa implementa é parcial. De fato, toda função convencional, definida para todas as entradas, é parcial também (veja o "pode não estar definida" na definição). E uma função parcial pode não estar definida para nenhum elemento do domínio. A função implementada pela subrotina abaixo se encaixa neste caso.

```
int loop(int n) {
  while ( 1 )
    ;
}
```

Definição 5.29. Seja B um subconjunto de A. A função $\chi_B : A \longrightarrow \{0, 1\}$ tal que

$$\chi_B(x) = \begin{cases} 1 & \text{se } x \in B \\ 0 & \text{se } x \notin B \end{cases}$$

é chamada de **função característica** de B.

[4] Assumindo um computador ideal com infinita memória.

5.6 Relações de Equivalência

Uma relação $R \subset A \times A$ é chamada de **relação de equivalência** se for:

reflexiva para todo $x \in A$, $x \, R \, x$;

simétrica para todo par $x, y \in A$, se $x \, R \, y$, então $y \, R \, x$;

transitiva para toda tripla $x, y, z \in A$, se $x \, R \, y$ e $y \, R \, z$, então $x \, R \, z$.

Note que todo $x \in A$ se relaciona com pelo menos um outro elemento de A, pois $x \, R \, x$.

Em notação de teoria dos conjuntos, em uma estrutura $\mathfrak{A} = \langle X, R \rangle$, onde $A \subset X$, R é uma relação de equivalência se as três fórmulas dadas a seguir são verdadeiras em $\mathfrak{A}$.

$$\forall x \, (x \in A \longrightarrow x \, R \, x)$$

$$\forall x \forall y \, (x \, R \, y \longrightarrow y \, R \, x)$$

$$\forall x \forall y \forall z \, (x \, R \, y \wedge y \, R \, z \longrightarrow x \, R \, z)$$

Exemplo 5.29. Considere que A é um conjunto de pessoas e $R \subset A^2$ é a relação tal que $a \, R \, b$ se e somente se a e b têm o mesmo nome. Então R é uma relação de equivalência pois é:

reflexiva cada pessoa tem um nome igual ao de si mesma;

simétrica se pessoa x tem nome igual ao da pessoa y, y tem nome igual ao de x;

transitiva se x tem nome igual a y e y tem nome igual a z, então x tem nome igual a z.

Exemplo 5.30. Considere A é o conjunto dos dias de um ano fixado e $R \subset A^2$ tal que $a \, R \, b$ se e somente se a e b forem no mesmo dia da semana. Então R é uma relação de equivalência pois é:

reflexiva um dado dia cai no mesmo dia da semana que si mesmo;

simétrica se o dia x cai no mesmo dia da semana que o dia y, y cai no mesmo dia da semana que x;

transitiva se o dia x cai no mesmo dia da semana que o dia y e y cai no mesmo dia da semana que o dia z, então x cai no mesmo dia da semana que o dia z.

Exemplo 5.31. Seja $R \subset \mathbb{Z}^2$ tal que $x \, R \, y$ se $x \equiv y \pmod{n}$ para um inteiro n fixado. Então, a relação de congruência R é uma relação de equivalência pois é:

reflexiva Dado $x \in \mathbb{Z}$, $x \, R \, x$, pois $x - x = 0 = 0n$;

simétrica Dados $x, y \in \mathbb{Z}$, se $x \, R \, y$, então $x - y = kn$ para algum inteiro k. Logo $y - x = (-k)n = dn$, onde $d = -k$ é inteiro. Portanto, temos $y \, R \, x$;

transitiva Dados $x, y, z \in \mathbb{Z}$, se $x \, R \, y$ e $y \, R \, z$, então $x - y = kn$ e $y - z = jn$ para inteiros k e j apropriados. Logo $x - z = x - y + y - z = (k + j)n = dn$, onde $d = k + j$ é inteiro. Portanto, temos $x \, R \, z$.

Exemplo 5.32. Seja Σ o conjunto de todos os símbolos da tabela ASCII. Usamos Σ^* para o conjunto de todas as cadeias de caracteres tomados de Σ (veja o exemplo 2.3). Então

$$\Sigma^* = \{\epsilon, a, b, c, \ldots, aa, ab, ac, \ldots, aaa, aab, aac, \ldots\}$$

Uma função qualquer $f : \Sigma^* \longrightarrow \mathbb{N}$ induz a uma relação R de equivalência entre cadeias de caracteres da seguinte forma:

$$x \, R \, y \text{ sse } f(x) = f(y) \text{ para } x, y \in \Sigma^*$$

Quando $f(x) \leqslant k$ para uma constante k, a função f pode ser utilizada como uma função *hash*, utilizada em uma estrutura de dados chamada de tabela *hash*. Em um dos tipos de tabela *hash*, todos os elementos de uma mesma classe de equivalência que são inseridos na tabela ficam agrupados em uma mesma lista encadeada. Elementos de listas diferentes pertencem a classes de equivalência diferentes.

Daremos um exemplo de como poderia ser f em uma linguagem de programação.

```
   // C/C++
int f(char *s) {
   int n = 0;
   while ( *s != '\0' )
      n = n + *s++*7;
   return n%k;
}
```

Note que `n%k` produz um valor entre 0 e $k-1$. Esta é a operação módulo, o resto da divisão de `n` por `k`.

Observação importante: relações de equivalência eliminam diferenças irrelevantes entre elementos tornando-os iguais na relação. Elas abstraem as informações relevantes para o nosso objetivo dentre todas as informações dos elementos. Por exemplo, no Exemplo 5.30, dois dias do ano são considerados "iguais" se tiverem o mesmo dia da semana. Então abstraimos o número do dia de duas datas, com 28 de abril e 22 de dezembro, e as consideramos como iguais (ambas são segundas-feiras em 2008).

Definição 5.30. Seja $A \neq \emptyset$ e $R \subset A^2$ uma relação de equivalência em A. Definimos

$$[x] = \{y \in A : x \, R \, y\}$$

Ou seja, $[x]$ contém todos os elementos relacionados a x. Como $x \, R \, x$, $x \in [x]$. E se $y \in [x]$ e $y \, R \, z$, temos $x \, R \, y$ e $y \, R \, z$. Logo $x \, R \, z$ e $z \in [x]$. Quando houver ambigüidade sobre qual relação está sendo utilizada, usamos $[x]_R$ ao invés de $[x]$.

Claramente, $x \in [x]$, pois $x \, R \, x$.

Proposição 5.4. *Seja $A \neq \emptyset$, R uma relação de equivalência em A e x e y quaisquer elementos de A. Então:*

(a) *$a \, R \, b$ se e somente se $[a] = [b]$*

(b) *$(a, b) \notin R$ se e somente se $[a] \cap [b] = \emptyset$.*

Demonstração. **(a)** ($\Longrightarrow$) Por hipótese, $a \, R \, b$. Provaremos que $[a] \subset [b]$ e $[b] \subset [a]$. Para todo $x \in [a]$, temos $a \, R \, x$ e $x \, R \, a$. De $x \, R \, a$ e $a \, R \, b$, pela transitividade concluímos que $x \, R \, b$. Por simetria, $b \, R \, x$; logo $x \in [b]$. Da mesma forma, para todo $x \in [b]$, $x \in [a]$. Portanto, $[a] = [b]$.

($\Longleftarrow$) Por hipótese, $[a] = [b]$. Como $a \in [a]$, $a \in [b]$. Assim, $b \, R \, a$ e, por simetria $a \, R \, b$.
(b) ($\Longrightarrow$) Temos o caso $X \longrightarrow Y$ onde X é "$(a, b) \notin R$" e Y" é "$[a] \cap [b] = \emptyset$". Isto é, $\neg X \vee Y$. Provaremos que a negação de $\neg X \vee Y$; isto é, $X \wedge \neg Y$, leva a uma contradição. Assuma que $(a, b) \notin R$ e $[a] \cap [b] \neq \emptyset$. Então há um elemento $x \in [a] \cap [b]$. Logo $a \, R \, x$ e $b \, R \, x$. Portanto, $a \, R \, x$ e $x \, R \, b$ (pela simetria) e $a \, R \, b$ pela transitividade. Logo, $(a, b) \in R$, uma contradição.

($\Longleftarrow$) Assumiremos $[a] \cap [b] = \emptyset$ e a negação de "$(a, b) \notin R$" e chegaremos a uma contradição. Então $(a, b) \in R$ e $b \in [a]$ pela definição do conjunto $[a]$. Como $b \in [b]$, $b \in [a] \cap [b]$. Contradição, pois $[a] \cap [b] = \emptyset$.

□

Proposição 5.5. *Toda relação de equivalência R no conjunto A produz uma partição e vice-versa.*

Demonstração. ($\Longrightarrow$) A partição criada pela relação de equivalência R é $P = \{[x] : x \in A\}$, onde $[x] = [x]_R$. Claramente P é uma partição, pois para todo $x \in A$, $x \in [x]$ (todo x pertence a alguma partição). E, dados dois conjuntos $[x]$ e $[y]$ da partição tais que $[x] \neq [y]$, temos pela Proposição 5.4(a) que $(x, y) \notin R$ e pela Proposição 5.4(b) qye $[x] \cap [y] = \emptyset$.

($\Longleftarrow$) A relação de equivalência de uma partição $P = \{P_1, P_2, \ldots, P_n\}$ de A é dada pela seguinte relação: $a \, R \, b$ sse a, b pertencem ambos a uma mesma parte P_i de P. Confira que esta relação é de equivalência. □

Definição 5.31. A partição de um conjunto A induzida por uma relação de equivalência R é chamada de **conjunto quociente** de A por R e denotada por

$$A/R = \{[x] : x \in A\}$$

Definição 5.32. Dado $n \in \mathbb{N}, n \geqslant 2$, o conjunto $\mathbb{Z}_n$ é definido como o conjunto quociente $\mathbb{Z}/R$ na qual R é a relação

$$a \, R \, b \text{ sse } a \equiv b \pmod{n}$$

Isto é, a e b pertencem à mesma classe de equivalência se ambos deixam o mesmo resto quando divididos por n.

As classes de equivalência de $\mathbb{Z}_n$ são denotadas por $\overline{0}, \overline{1}, \overline{2}, \ldots \overline{n-1}$ sendo que $\overline{i}$ contém todos os elementos de $\mathbb{Z}$ que deixam resto i quando divididos por n. Estude os exemplos abaixo.

Exemplo 5.33. $a \equiv b \pmod 2$ se e somente se $a - b = 2k$. Se a e b forem inteiros, ambos devem ser pares ou ambos devem ser ímpares (confira). Isto é, $a \equiv b \pmod 2$ se e somente se ambos deixam resto 0 na divisão por 2 ou ambos deixam resto 1.

Pela definição,

$$\begin{aligned} \mathbb{Z}_2 &= \{\{0, 2, -2, 4, -4, \ldots\}, \{1, -1, 3, -3, \ldots\}\} \\ \mathbb{Z}_2 &= \{\overline{0}, \overline{1}\} \end{aligned}$$

Sendo $\overline{0} = \{0, 2, -2, 4, -4, \ldots\}$ e $\overline{1} = \{1, -1, 3, -3, \ldots\}$. Então $2 \in \overline{0}$ e $5, -7 \in \overline{1}$. Todo número inteiro n pode ser escrito como $n = 2q$ ou $n = 2q+1$. Os primeiros são os pares e pertencem a $\overline{0}$. Os segundos são os ímpares e pertence a $\overline{1}$.

Exemplo 5.34. Seja $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Então $2, 7 \in \overline{2}$ pois $2 = 0 \cdot 5 + 2$ e $7 = 1 \cdot 5 + 2$.

Definição 5.33. A adição, subtração e multiplicação de elementos de $\mathbb{Z}_n$ é definida como se segue:

(a) $\overline{a} + \overline{b} = \overline{a + b}$.

(b) $\overline{a} - \overline{b} = \overline{a - b}$.

(c) $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

O conjunto $\mathbb{Z}_n$ com estas operações forma uma estrutura $\langle \mathbb{Z}_n, +, -, \cdot \rangle$ com muitas propriedades interessantes, com larga aplicação na Matemática e Computação.

Duas propriedades de $\mathbb{Z}_n$ são:

(a) para $0 \leqslant i < n$, $i \in \overline{i}$ pois $i = 0 \cdot n + i$, o resto da divisão de i por n é i;

(b) $\overline{n} = \overline{0}$ (logo $\overline{n + k} = \overline{n} + \overline{k} = \overline{0} + \overline{k} = \overline{0 + k} = \overline{k}$)

O conjunto $\mathbb{Z}_n$ pode ser representado por um círculo no qual o sucessor do último elemento, $\overline{n-1}$ é $\overline{0}$. Assim, $\overline{n-1} + \overline{1} = \overline{0}$. E $\overline{n-1} + \overline{2} = \overline{1}$.

Exercícios

5.33. Prove que a relação definida no exemplo 5.32 é uma relação de equivalência.

5.34. Prove que a relação definida a partir de uma partição, na Proposição 5.5, é de equivalência.

5.35. Encontre o erro na seguinte prova de que toda relação simétrica e transitiva é também reflexiva.
Afirmação: se R é simétrica e transitiva, então R é reflexiva.
Prova: dado $(a, b) \in R$, temos $(b, a) \in R$ pois R é simétrica. Então de $(a, b), (b, a) \in R$, pela transitividade, concluimos que $(a, a) \in R$. Logo R é reflexiva.

5.36. Mostre que são relações de equivalência:

(a) a relação sobre o conjunto de triângulos tal que dois elementos são equivalentes se eles são congruentes (todos os ângulos iguais);

(b) a relação $\equiv$ de equivalência lógica entre sentenças do cálculo proposicional;

(c) $R \subset \mathbb{N}^2 \times \mathbb{N}^2$ tal que $(a, b)\ R\ (c, d)$ se e somente se $a + d = b + c$;

(d) a relação $r\ R\ s$ se a reta r é paralela à reta s. Utilize o conjunto de todas as retas em um plano.

5.37. Mostre que **não** são relações de equivalência:

(a) a relação $\subset$ entre conjuntos;

(b) a relação $\leqslant \subset \mathbb{R}^2$ que compara dois números reais;

(c) a relação $\in$ entre conjuntos.

5.38. Prove as seguintes propriedades da congruência.

(a) se $a \equiv b \pmod{n}$, então $a + c \equiv b + c \pmod{n}$;

(b) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$;

(c) se $a \equiv b \pmod{n}$, então $ac \equiv bc \pmod{n}$;

(d) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $ac \equiv bd \pmod{n}$.

(e) $a \equiv b \pmod{0}$ sse $a = b$;

(f) para quaisquer $a, b \in \mathbb{Z}$, $a \equiv b \pmod{1}$;

(g) $a \equiv b \pmod{n}$ sse $a \equiv b \pmod{-n}$.

5.39. Se hoje for terça-feira e este ano não for bissexto, qual o dia da semana deste mesmo dia do mês no próximo ano?

5.40. Que dia da semana é terça-feira + quinta-feira? E segunda-feira $\cdot$ sexta-feira? Lembre-se de que a semana começa no domingo. Defina operações de soma e multiplicação razoáveis para dias da semana.

5.41. Se agora são 21h e 37 minutos, a que horas serão daqui a 13h e 54 minutos?

5.7 Relações de Ordem

Conjuntos são utilizados extensivamente na Matemática e na Computação. Freqüentemente é necessário que os elementos do conjunto estejam ordenados de alguma forma. Por exemplo,

- os números naturais estão ordenados em $0, 1, 2, 3, \ldots$. Utilizamos fatos como $n < n+1$ extensivamente nas provas Matemáticas;
- os conjuntos estão ordenados pela relação $\subset$. Podemos considerar $A < B$ se $A \subset B$;
- o conjunto das câmeras fotográficas de uma loja podem estar ordenados pelos seus preços, do menor para o maior;
- o conjunto das árvores binárias completas (alturas iguais, cada vértice com zero ou dois filhos) podem estar ordenados por número de vértices;
- o conjunto dos componentes necessários para montar certa máquina (exemplo: um micro-ondas, um carro, avião, etc) podem estar ordenados pela ordem em que eles devem ser montados. Não se pode, por exemplo, colocar as rodas no carro antes de colocar o chassis. Ou colocar o rádio antes de ter colocado o painel.

Definição 5.34. Um **conjunto parcialmente ordenado** (*partially ordered set*, *poset*) é uma estrutura $\langle S, \preceq \rangle$ onde S é um conjunto e $\preceq$ é uma relação binária reflexiva, anti-simétrica e transitiva. Isto é, para quaisquer elementos $a, b, c \in S$, temos

reflexiva $a \preceq a$

anti-simétrica $a \preceq b$ e $b \preceq a$ implica em $a = b$

transitiva $a \preceq b$ e $b \preceq c$ implica em $a \preceq c$

Note que um *poset* é um conjunto com uma operação. De fato, uma estrutura. Na definição da estrutura, utilizamos o símbolo $\preceq$ para a relação. Mas uma estrutura real da Matemática pode utilizar um símbolo diferente para a relação — veja nos exemplos abaixo.

Exemplo 5.35. Há inúmeros exemplos de conjuntos parcialmente ordenados na Matemática e na Computação:

1. os números reais com a comparação $\leqslant$. A estrutura $\langle \mathbb{R}, \leqslant \rangle$ é um *poset*. Vejamos: para todo $x, y, z \in \mathbb{R}$, $x \leqslant x$, $x \leqslant y$ e $y \leqslant x$ implica em $x = y$ e $x \leqslant y$ e $y \leqslant z$ implica em $x \leqslant z$;
2. o conjunto dos subconjuntos de um conjunto S, $\mathcal{P}(S)$ ou 2^S, com a relação $\subset$. A estrutura é $\langle 2^S, \subset \rangle$. Vejamos: para todo $A, B, C \in \mathcal{P}(S)$, $A \subset A$, $A \subset B$ e $B \subset A$ implica em $A = B$ (definição de igualdade entre conjuntos) e $A \subset B$ e $B \subset C$ implica em $A \subset C$;

3. os números naturais com a relação D tal que $n\ D\ m$ sse n divide p (existe $k \in \mathbb{N}$ tal que $n \cdot k = p$). Então $n\ D\ n$, $n\ D\ m$ e $m\ D\ n$ implica em $n = m$ e $n\ D\ m$ e $m\ D\ p$ implica em $n\ D\ p$;

4. para construir a tabela verdade para uma fórmula como $\phi =_{def} (A \longrightarrow B) \wedge (\neg B \vee C) \longrightarrow C$, construimos tabelas auxiliares para cada sub-fórmula desta fórmula. E cada sub-fórmula pode ter outras sub-fórmulas até que se chegue na fórmula mais simples que é uma única variável. Assim, as sub-fórmulas de ϕ são C e $(A \longrightarrow B) \wedge (\neg B \vee C)$. As sub-fórmulas desta última são $(A \longrightarrow B)$ e $(\neg B \vee C)$. As sub-fórmulas de $A \longrightarrow B$ são A e B. As de $\neg B \vee C$ são $\neg B$ e C. E a sub-fórmula de $\neg B$ é B. Assim, existe uma relação de ordem entre estas fórmulas: $X \prec Y$ sse X é sub-fórmula de Y. Então:

$C \prec (A \longrightarrow B) \wedge (\neg B \vee C) \longrightarrow C$	$(A \longrightarrow B) \wedge (\neg B \vee C) \prec (A \longrightarrow B) \wedge (\neg B \vee C) \longrightarrow C$
$A \longrightarrow B \prec (A \longrightarrow B) \wedge (\neg B \vee C)$	$\neg B \vee C \prec (A \longrightarrow B) \wedge (\neg B \vee C)$
$A \prec A \longrightarrow B$	$B \prec A \longrightarrow B$
$\neg B \prec \neg B \vee C$	$C \prec \neg B \vee C$
$B \prec \neg B$	

Em um conjunto parcialmente ordenado, dois elementos a e b são **comparáveis** se estão relacionados de alguma forma, isto é, ou $a \preceq b$ ou $b \preceq a$. Nem todos os elementos são comparáveis em um conjunto parcialemnte ordenado. Por exemplo, considere a estrutura formada pelo conjunto $\{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ das partes de $\{0,1\}$ com a relação $\subset$. Não temos $\{0\} \subset \{1\}$ ou $\{1\} \subset \{0\}$. Estes elementos não são comparáveis. Mas outros são, como $\emptyset \subset \{0\}$ e $\{1\} \subset \{0,1\}$.

Definição 5.35. Podemos definir mais precisamente, em termos de lógica, o que é um conjunto parcialmente ordenado. Uma estrutura $\mathfrak{A} = \langle S, \preceq \rangle$ é um conjunto parcialmente ordenado se ela é modelo para as seguintes fórmulas:

$$\forall a\ (a \preceq a)$$
$$\forall a \forall b\ (a \preceq b \wedge b \preceq a \longrightarrow a = b)$$
$$\forall a \forall b \forall c\ (a \preceq b \wedge b \preceq c \longrightarrow a \preceq c)$$

Se Γ é o conjunto destas três fórmulas, então $\mathfrak{A}$ é um conjunto parcialmente ordenado se $\mathfrak{A} \models \Gamma$. Isto é, se $\mathfrak{A}$ é um modelo para Γ.

Definição 5.36. Um **conjunto totalmente ordenado** (*totally ordered set*) é uma estrutura $\langle S, \preceq \rangle$ onde S é um conjunto e $\preceq$ é uma relação binária reflexiva, anti-simétrica, transitiva e total. Isto é, para quaisquer elementos $a, b, c \in S$, temos

reflexiva $a \preceq a$

anti-simétrica $a \preceq b$ e $b \preceq a$ implica em $a = b$

transitiva $a \preceq b$ e $b \preceq c$ implica em $a \preceq c$

total ou $a \preceq b$ ou $b \preceq a$

Escrevemos "O conjunto S é totalmente ordenado pela relação $\preceq$" ou "S tem uma ordem total", deixando implícita a relação utilizada.

Uma ordem total é então uma ordem parcial onde todos os elementos são comparáveis. Note que se uma relação de ordem é total, ela é reflexiva, pois cada elemento deve ser comparável a todos os outros, o que inclui a si mesmo.

Exemplo 5.36. São exemplos de estruturas totalmente ordenados:

(a) $\langle \mathbb{R}, \leqslant \rangle$, todos os elementos dos reais são comparáveis;

(b) o conjunto $\{\emptyset, \{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}\}$ com a relação $\subset$

(c) o conjunto das letras maiúsculas do alfabeto com a ordem alfabética: $A \leqslant B$, $B \leqslant C$, etc;

(d) $\langle S, \subset \rangle$, onde $S = \bigcup_{i \in \mathbb{N}} \{\{\{n \in \mathbb{N} : n \leqslant i\}\}\}$. Verifique porque utilizamos conjunto dentro de conjunto na definição de S;

Definição 5.37. Um **conjunto estritamente totalmente ordenado** (*strict total order*) é uma estrutura $\langle S, \prec \rangle$ onde S é um conjunto e $\prec$ é uma relação binária assimétrica, transitiva e que obedece à lei da tricotomia. Isto é, para quaisquer elementos $a, b, c \in S$, temos

assimétrica $a \prec b$ implica em $b \not\prec a$

transitiva $a \prec b$ e $b \prec c$ implica em $a \prec c$

lei da tricotomia exatamente uma de três coisas é verdadeira: $a \prec b$, $b \prec a$ ou $a = b$.

Definição 5.38. Uma relação $R \subset A \times B$ é irreflexiva se para todo $a \in A$, $a \not R a$.

Exercícios

5.42. Verifique se as seguintes estruturas são ordens parciais, totais ou nenhuma delas.

(a) $\langle S, \subset \rangle$ no qual $S \subset 2^{\mathbb{R}}$, $S = \{(a, b) : a, b \in \mathbb{N}\}$;

(b) $\langle S, \subset \rangle$ no qual $S \subset 2^{\mathbb{R}}$, $S = \{(\frac{-1}{n}, \frac{1}{n}) : n \in \mathbb{N}^*\}$;

(c) $\langle G, R \rangle$ no qual G é um grafo acíclico dirigido e R é a relação de alcançabilidade (*reachability*). Isto é, $x \; R \; y$ se e somente se há um caminho de x para y.

5.43. Para cada ítem abaixo, encontre uma relação:

(a) reflexiva e transitiva;

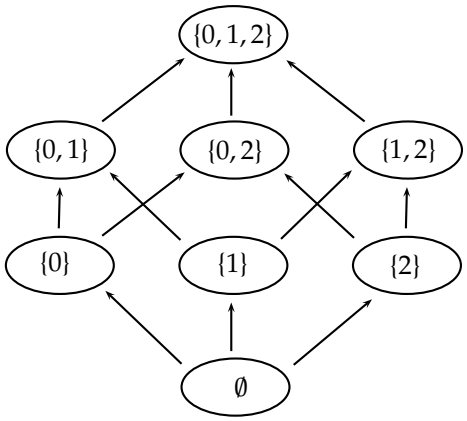


Figura 5.6: Diagrama de Hasse do *poset* formado pelos subconjuntos de $\{0, 1, 2\}$ e a relação $\subset$

(b) assimétrica e irreflexiva;

(c) não reflexiva e não irreflexiva;

(d) que não é reflexiva mas que contém um subconjunto reflexivo (subconjunto da relação original).

5.44. Sobre uma relação R sobre um conjunto S, prove:

(a) se R é assimétrica, R é irreflexiva;

(b) se R é assimétrica, R é anti-simétrica;

5.8 Diagramas de Hasse

Um diagrama de Hasse é uma representação gráfica dos elementos de um conjunto parcialmente ordenado e da relação de ordem entre eles. Dada uma estrutura $\langle S, \preceq \rangle$ que é um conjunto parcialmente ordenado e finito, o diagrama de Hasse para esta estrutura é construído da seguinte forma: desenha-se cada elemento do conjunto S e liga-se por um segmento de reta o elemento x a y se $x \preceq y$ e não existe um $z \in S$ tal que $x \preceq z$ e $z \preceq y$. O elemento x é colocado abaixo de y no diagrama.

Exemplo 5.37. A Figura 5.6 mostra o diagrama de Hasse do conjunto parcialmente ordenado formado pelos subconjuntos de $\{0, 1, 2\}$ e pela relação $\subset$. O conjunto utilizado é então:

$$\{\emptyset,\ \{0\},\ \{1\},\ \{2\},\ \{0, 1\},\ \{0, 2\},\ \{1, 2\},\ \{0, 1, 2\}\}$$

5.9 Teoria Axiomática dos Conjuntos

A teoria vista anteriormente é a teoria ingênua dos conjuntos. Ela permite paradoxos como o de Russel . A teoria axiomática que estudaremos, a de Zermelo-Fraenkel, foi cuidadosamente projetada durante décadas para eliminar qualquer possibilidade de paradoxos ou inconsistências. Esta teoria é chamada de ZF e utiliza seis axiomas [3]. Estes axiomas mais o axioma da escolha (A7 abaixo) constituem-se na teoria ZFC que é base para formalizar toda a Matemática. A partir desta teoria pode-se deduzir todos os axiomas sobre os números naturais, desde que os símbolos $+$, $\cdot$, $'$ e 0 sejam representados de uma certa forma (não mostrada) utilizando-se somente o símbolo $\in$. Aliás, este é o único predicado utilizado pelos axiomas. Funções e constantes não são necessários. Contudo, para facilitar o entendimento dos axiomas, utilizaremos o conjunto vazio, $\emptyset$, como constante. Nos comentários a respeito das fórmulas, interpretamos as fórmulas dadas em um modelo da teoria dos conjuntos.

A1 $\forall z\,(z \in x \longleftrightarrow z \in y) \longrightarrow (x = y)$, axioma da extensionalidade. Este axioma significa o seguinte: se x e y têm os mesmos elementos, eles são iguais;

A2 $F_\varphi \longrightarrow (\exists b\,\forall y\,(y \in b \longleftrightarrow \exists x\,(x \in a \wedge \varphi(x, y))))$, axioma da substituição. F_φ é a fórmula $\forall x\,\forall y\,\forall z\,(\varphi(x,\, y) \wedge \varphi(x,\, z) \longrightarrow (y = z))$. Este axioma garante que podemos construir um conjunto b que seja a imagem de uma fórmula φ que é usada como uma função tendo a como domínio;

A3 $\exists y\,\forall x\,(x \in y \longleftrightarrow \forall z\,(z \in x \longrightarrow z \in a))$, axioma das partes. Este axioma garante que existe o conjunto das partes de um conjunto a se a existe;

A4 $\exists y\ \forall y\ (x \in y \longleftrightarrow \exists z\ (x \in z \wedge z \in a))$, axioma da reunião. Este axioma garante a existência de um conjunto que é a união de todos elementos de a. Naturalmente, na interpretação deste axioma na teoria dos conjuntos usuais, a é composto de conjuntos. Em outras palavras, este axioma garante a existência de $\{x : \exists z\,(x \in z \wedge z \in a)\}$;

A5 $\exists y\,(y \in x) \longrightarrow \exists y\,(y \in x \wedge \forall z \neg(z \in x \wedge z \in y))$, axioma da regularidade. Este axioma garante que um conjunto não está contido em si mesmo direta ou indiretamente. Este é o mais complexo de todos os axiomas de ZF;

A6 $\exists w\,((\emptyset \in w) \wedge \forall x\,(x \in w \longrightarrow x \cup \{x\} \in w))$, axioma da infinidade. Este axioma garante a existência de um conjunto infinito. A saber, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \ldots\}$. O símbolo $\cup$ é um meta-predicado. $x \cup y$ é uma abreviação de $\exists z\,(w \in z \longleftrightarrow (w \in x \vee w \in y))$;

A7 $(\forall x\,(x \in z \longrightarrow \neg(x = \emptyset)) \wedge (\forall x\,\forall y\,(x \in z \wedge y \in z \wedge \neg(x = y)) \longrightarrow (x \cap y = \emptyset))) \longrightarrow \exists u\,\forall x\,\exists v\,(x \in z \longrightarrow u \cap x = \{v\})$, axioma da escolha. O símbolo $\cap$ é um meta-predicado. $x \cap y$ significa $\exists z\,(w \in z \longleftrightarrow (w \in x \wedge w \in y))$.

Este axioma garante que, dado um conjunto z que possui como elementos outros conjuntos, existe um conjunto u tal que u possui exatamente um elemento em comum com cada elemento de z (que é um conjunto). Exige-se que os elementos de z não

sejam vazios e que dois a dois não tenham elementos em comum. Estudando a fórmula,

1. $\forall x\ (x \in z \longrightarrow \neg(x = \emptyset))$ garante que todos os elementos de z sejam diferentes de $\emptyset$;
2. $(\forall x\ \forall y\ (x \in z \wedge y \in z \wedge \neg(x = y)) \longrightarrow (x \cap y = \emptyset))$ garante que quaisquer dois elementos de z, que são conjuntos, tem intersecção vazia;
3. $\exists u\ \forall x\ \exists v\ (x \in z \longrightarrow u \cap x = \{v\})$ garante que existe u que tem exatamente um elemento v em comum com cada elemento x de z dado que os itens 1 e 2 acima, quando interpretados, são verdadeiros. Como $\exists v$ aparece depois de $\exists x$, para cada x de z podemos ter um elemento v diferente — de fato, todos eles são diferentes, já os elementos de z são dois a dois disjuntos.

5.10 Cardinalidade

Esta seção discorre sobre conjuntos infinitos e a relação entre eles. Alguns dos resultados trazem profundas conseqüências para a Computação. A saber, que há mais funções dos naturais para os naturais do que programas de computadores para calculá-las. Em resumo, há mais problemas no mundo do que programas de computador para resolvê-los. Para chegar a este resultado, é necessário comparar conjuntos infinitos em relação ao "tamanho". Mas como isto é possível? Se dois conjuntos são infinitos, como $\mathbb{N}$ e $\mathbb{R}$, um não pode ter mais elementos do que o outro. Afinal, se formos enumerando os elementos, jamais terminaríamos nenhum deles. Contudo, esta comparação é possível — veja a próxima definição.

Definição 5.39. Um conjunto A será **equipotente** ou **equipolente** a um conjunto B se existir uma função bijetora $f : A \longrightarrow B$. Utilizaremos $A \sim B$ se A for equipotente a B.

Exemplo 5.38. O conjunto $A = \{0, 1, 2\}$ é equipotente ao conjunto $B = \{10, 11, 12\}$. A função bijetora f é facilmente definível como $f(n) = 10 + n$. Se os conjuntos A e B forem finitos e possuírem o mesmo número de elementos, sempre será possível construir uma função f bijetora entre eles. Mas espere ... ainda não definimos "conjunto finito"!

Exemplo 5.39. O conjunto dos pares positivos $P = \{0, 2, 4, 6, \ldots\}$ é equipotente ao conjunto dos ímpares positivos $I = \{1, 3, 5, \ldots\}$. A função $f : P \longrightarrow I$ dada por $f(n) = n + 1$ é bijetora.

Exemplo 5.40. O conjunto dos pares positivos $P = \{0, 2, 4, 6, \ldots\}$ é equipotente a $\mathbb{N}$ pela função bijetora $f : \mathbb{N} \longrightarrow P$ dada por $f(n) = 2n$.

Proposição 5.6. *Um intervalo real (a, b) é equipotente a $(0, 1)$. E para quaisquer dois intervalos (a, b) e (c, d), temos $(a, b) \sim (c, d)$.*

Demonstração. Imagine a reta que passa pelos pontos $(0, a)$ e $(1, b)$. Há uma correspondência um a um entre as coordenadas $x \in (0, 1)$ e as ordenadas $y \in (a, b)$. A função que relaciona os conjuntos é:

$$f : (0, 1) \longrightarrow (a, b) \text{ tal que } f(x) = a + (b - a)x$$

Da mesma forma, qualquer intervalo (a, b) é equipotente a qualquer outro intervalo (c, d). A função que relaciona biunivocamente os conjuntos é:

$$f : (a, b) \longrightarrow (c, d) \text{ tal que } f(x) = c + (x - a)\frac{d - c}{b - a}$$

□

Proposição 5.7. *A relação $\sim$ entre conjuntos é uma relação de equivalência.*

Demonstração. Todo conjunto A é equipotente a ele mesmo. Use a função $f(x) = x$. É bijetora. Se $A \sim B$, existe $f : A \longrightarrow B$ bijetora. Toda bijetora tem inversa bijetora. Logo existe $f^{-1} : B \longrightarrow A$ bijetora. Se $A \sim B$ e $B \sim C$, existem $f : A \longrightarrow B$ e $g : B \longrightarrow C$ bijetoras. Como composição de bijetoras é bijetora, existe $g \circ f : A \longrightarrow C$ bijetora e $A \sim C$.

□

Proposição 5.8. *Um conjunto A será chamado de* **infinito** *se existir uma função $f : A \longrightarrow A$ injetora mas não sobrejetora. Em outras palavras, existe um subconjunto próprio B de A tal que existe uma função $g : A \longrightarrow B$ bijetora. Logo B é $Im(f)$ com $g(x) = f(x)$ para todo $x \in A$.*

Proposição 5.9. *Um conjunto A será chamado de* **finito** *se não for infinito. Isto é, não existe uma função $f : A \longrightarrow A$ injetora mas não sobrejetora.*

Proposição 5.10. *O conjunto $\mathbb{N}$ é infinito. Tome $f : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(n) = n + 1$. Esta função é injetora mas não sobrejetora, pois $0 \notin Im(f)$.*

Exemplo 5.41. O conjunto $\{0, 1\}$ é finito.

Proposição 5.11. *Para todo conjunto finito $A \neq \emptyset$ existe um $k \in \mathbb{N}$ tal que $A \sim \{1, 2, \ldots k\}$.*

Exemplo 5.42. Seja $A = \{\diamond, \spadesuit, \sharp, \bigstar\}$. Então $A \sim \{1, 2, 3, 4\}$. Tome f tal que $f(1) = \diamond$, $f(2) = \spadesuit$, $f(3) = \sharp$ e $f(4) = \bigstar$.

Proposição 5.12. *O conjunto (a, b) é equipotente a $\mathbb{R}$.*

Demonstração. O conjunto $(-1, 1)$ é equipotente ao conjunto $\mathbb{R}$. Confira que a função $f : (-1, 1) \longrightarrow \mathbb{R}$ definida abaixo é bijetora.

$$f(x) = \begin{cases} 0 & \text{se } x = 0 \\ \frac{1-|x|}{x} & \text{se } x \neq 0 \end{cases}$$

Esta função é $f(x) = \frac{1}{x} - 1$ se $x \in (0, 1)$, $f(x) = \frac{1}{x} + 1$ se $x \in (-1, 0)$ e $f(0) = 0$. Pela Proposição 5.6, $(a, b) \sim (-1, 1)$. Como provamos que $(-1, 1) \sim \mathbb{R}$, temos $(a, b) \sim \mathbb{R}$. □

Definição 5.40. Um conjunto é **enumerável** se ele é finito ou é equipotente a $\mathbb{N}$. Um conjunto é **denumerável** se ele é equipotente a $\mathbb{N}$. Um conjunto enumerável pode ser colocado em correspondência um a um ou com um conjunto $\{0, 1, 2, \ldots k\}$ ou com $\mathbb{N}$. Em qualquer caso, podemos listar os elementos do conjunto enumerável A: $a_0, a_1, a_2, a_3, \ldots$.

Proposição 5.13. *Todo subconjunto de um conjunto enumerável é enumerável.*

Demonstração. Seja A um conjunto enumerável. Se A é finito, todo subconjunto de A será finito (prove!). Considere A infinito e seja $B \subset A$. Se B for finito, será enumerável. Suponha então que B seja infinito.

Como A é enumerável, $A = \{a_0, a_1, a_2, \ldots\}$. Dado um elemento $b \in B$, b é algum dos elementos a_i de A. Baseado nisto construiremos uma função $f : \mathbb{N} \longrightarrow B$ que é bijetora. Seja a_{i_0} o primeiro elemento de A que pertence a B (isto é, $a_i \notin B$ para $i < i_0$). Faça $f(0) = a_{i_0}$. Seja a_{i_1} o primeiro elemento de A que pertence a B. Faça $f(1) = a_{i_1}$ e assim por diante. Então se $f(n) = a_{i_n}$, há n elementos de B no conjunto $\{a_0, a_1, \ldots a_{i_n}\}$.

Esta função é claramente bijetora. □

Corolário 5.1. *Todo subconjunto infinito de* $\mathbb{N}$ *é enumerável.*

Exemplo 5.43. O conjunto dos primos é enumerável. Seja P o conjunto dos números primos. Este conjunto é infinito pela Proposição 3.6 e subconjunto de $\mathbb{N}$. Pelo Corolário acima, P é enumerável. Encontraremos uma enumeração de P.

$$\begin{array}{cccccccccccccccccccc}
0, & 1, & 2 & , 3, & 4, & 5, & 6 & 7, & 8, 9, 10, & 11, & 12, & 13, & 14, 15, 16, & 17, & 18, & 19, & 20, 21, \ldots \\
 & & \uparrow & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & \\
 & & 0 & 1 & & 2 & & 3 & & 4 & & 5 & & 6 & & 7 &
\end{array}$$

Se um número p_i possui índice i na lista acima, então $f : \mathbb{N} \longrightarrow P$ é definida como $f(i) = p_i$.

Exemplo 5.44. O conjunto dos pares é enumerável. Neste caso, é fácil encontrar uma função $f : \mathbb{N} \longrightarrow P$ bijetora, onde P é o conjunto pares. Use $f(n) = 2n$.

Proposição 5.14. *Se A e B são enumeráveis, $A \cup B$ é enumerável.*

Demonstração. Faremos apenas o caso não trivial em que A e B são infinitos. Como A e B são enumeráveis, eles podem ser escritos da seguinte forma:

$$\begin{array}{cccccccc}
A = \{ & a_0, & a_1, & a_2, & a_3 & \ldots\} \\
 & \downarrow\nearrow & \downarrow\nearrow & \downarrow\nearrow & \downarrow\nearrow & \\
B = \{ & b_0, & b_1, & b_2, & b_3 & \ldots\}
\end{array}$$

As setas indicam como fazer uma função $f : \mathbb{N} \longrightarrow A \cup B$. Faça $f(0) = a_0$, $f(1) = b_0$, $f(2) = a_1$, $f(3) = b_1$ e assim por diante. □

Proposição 5.15. $\mathbb{N}$ *é equipotente a* $\mathbb{Z}$.

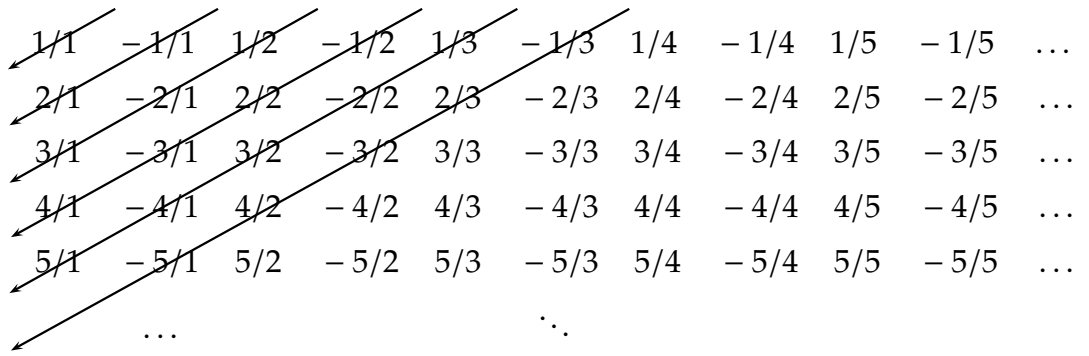


Figura 5.7: Uma relação bijetora entre $\mathbb{N}$ e $\mathbb{Q}$

Demonstração. Isto pode ser claramente verificado enumerando-se os elementos de $\mathbb{Z}$ da seguinte forma:

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$$

Uma função bijetora $f : \mathbb{N} \longrightarrow \mathbb{Z}$ é

$$f(n) = \begin{cases} \frac{(n+1)}{2} & \text{se } n \text{ é ímpar} \\ -\frac{n}{2} & \text{se } n \text{ é par} \end{cases}$$

□

Proposição 5.16. $\mathbb{N} \sim \mathbb{Q}$

Demonstração. Construiremos uma função $f : \mathbb{N} \longrightarrow \mathbb{Q}$ bijetora usando a tabela da Figura 5.7. As setas da tabela definem uma enumeração dos números racionais se seguirmos a direção dada pelas setas e seguindo da seta menor para as maiores. Esta enumeração é $1/1, -1/1, 2/1, 1/2, -2/1, \ldots$. Os valores de $f(1), f(2), f(3), \ldots$ são associados aos valores desta enumeração ($f(1) = 1/1$, por exemplo). E $f(0) = 0$. Números repetidos que aparecem na tabela não são considerados. Por exemplo, $f(8)$ deveria ser $2/2$, mas $2/2 = 1$ e já temos $f(1) = 1/1 = 1$. Então $f(8) = -3/1$.

Esta função é claramente bijetora e então $\mathbb{N} \sim \mathbb{Q}$.

□

Proposição 5.17. *Se A e B são enumeráveis, $A \times B$ é enumerável.*

Demonstração. Provaremos apenas no caso em que A e B são infinitos. Como A e B são enumeráveis, o conjunto $A \times B$ pode ser escrito da seguinte forma:

$$\begin{array}{cccc} (a_0, b_0) & (a_0, b_1) & (a_0, b_2) & (a_0, b_3) & \ldots \\ (a_1, b_0) & (a_1, b_1) & (a_1, b_2) & (a_1, b_3) & \ldots \\ (a_2, b_0) & (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \ldots \\ (a_3, b_0) & (a_3, b_1) & (a_3, b_2) & (a_3, b_3) & \ldots \\ (a_4, b_0) & (a_4, b_1) & (a_4, b_2) & (a_4, b_3) & \ldots \\ \ldots & & & & \end{array}$$

Podemos utilizar o argumento diagonal como foi utilizado para provar que $\mathbb{N} \sim \mathbb{Q}$. Isto é, $f : \mathbb{N} \longrightarrow A \times B$ é tal que

$$\begin{array}{cccccccc} n & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ f(n) & (a_0, b_0) & (a_0, b_1) & (a_1, b_0) & (a_0, b_2) & (a_1, b_1) & (a_2, b_0) & \dots \end{array}$$

□

Proposição 5.18. *O conjunto* $(0, 1) \times (0, 1)$ *é equipotente a* $(0, 1)$.

Demonstração. Escreveremos um número real $x \in (0, 1)$ como $0.x_0x_1x_2x_3 \ldots$. Construiremos uma função $f : (0, 1) \times (0, 1) \longrightarrow (0, 1)$ bijetora.

$$f(0.x_0x_1x_2x_3 \ldots, 0.y_0y_1y_2y_3 \ldots) = 0.x_0y_0x_1y_1x_2y_2x_3y_3 \ldots$$

Fica como exercício provar que esta função é bijetora (fácil).

Note que $(0, 1) \times (0, 1)$ é um quadrado no plano cartesiano. Este teorema diz que um quadrado é equipotente a um segmento aberto da reta.

□

Proposição 5.19. $\mathbb{N}$ *não é equipotente a* $\mathbb{R}$.

Demonstração. Provaremos por contradição: assumiremos que existe uma enumeração dos números reais, uma função $g : \mathbb{N} \longrightarrow \mathbb{R}$ bijetora. Como $(0, 1) \sim \mathbb{R}$, então suponha que exista $f : \mathbb{N} \longrightarrow (0, 1)$ bijetora. Isto é o mesmo que dizer que os números reais entre 0 e 1 podem ser colocados em uma lista $r_0, r_1, r_2, r_3, \ldots$, uma enumeração dos elementos do conjunto $(0, 1)$. Isto é, $f(0) = r_0$, $f(1) = r_1, \ldots$

Vamos colocar esta enumeração em uma tabela:

$$\begin{array}{cccccccc} r_0 & 0, & 1 & 2 & 1 & 7 & 9 & \dots \\ r_1 & 0, & 0 & 9 & 7 & 8 & 1 & \dots \\ r_2 & 0, & 6 & 4 & 0 & 0 & 2 & \dots \\ r_3 & 0, & 5 & 5 & 3 & 0 & 3 & \dots \\ r_4 & 0, & 7 & 8 & 8 & 2 & 1 & \dots \\ \vdots & & & & & & & \end{array}$$

Isto é, $r_0 = 0.12179 \ldots$, $r_1 = 0.09781 \ldots$ e assim por diante. Encontraremos um número $s = 0.s_0s_1s_2s_3 \ldots$ tal que s não está na listagem acima. Para tanto, suponha que r_{ij} seja o j-ésimo dígito depois da vírgula de r_i, $j \geqslant 0$. Isto é, $r_{00} = 1$, $r_{01} = 2$, $r_{02} = 1$, $r_{21} = 4$ e $r_{32} = 3$. O número s é definido, dígito a dígito, da seguinte forma:

$$s_j = \begin{cases} 0 & \text{se } r_{jj} \neq 0 \\ 1 & \text{se } r_{jj} = 0 \end{cases}$$

Portanto, o i-ésimo dígito de s é diferente do i-ésimo dígito de r_i, começando com $i = 0$. Então usando a tabela acima,

$$s = 0.00110 \ldots$$

s **é diferente em pelo menos um dígito de cada um dos elementos** r_i **enumerados na tabela acima**. Vejamos: s é diferente do número $r_0 = 0.1217\ldots$ pois $s_0 \neq r_{00}$. Da mesma forma, o segundo dígito de r_1 depois da vírgula, r_{11}, é diferente de s_1 e assim por diante. Então s não aparece nesta tabela, pois este número é diferente em pelo menos um dígito de qualquer número que aparece na tabela.

Concluindo, como $s = 0.s_0s_1s_2s_3\ldots$ e $s_i \neq r_{ii}$ para todo $i \in \mathbb{N}$, temos $s \neq r_i$ para todo i. Portanto construimos um número $s \in \mathbb{R}$ que não aparece na listagem $r_0, r_1, r_2, \ldots$.

Note que a função $f : \mathbb{N} \longrightarrow (0, 1)$ definida inicialmente nesta prova é tal que $f(i) = r_i$. Mas acabamos de mostrar que f não é sobrejetora. Logo, não é bijetora, uma contradição.

A técnica utilizada nesta prova é chamada de "diagonalização" de Cantor, sendo **muito importante** na Computação e na Lógica. □

Definição 5.41. Um conjunto Σ que contém símbolos é chamado de **alfabeto**.

Dado um alfabeto Σ, o conjunto $\Sigma^\star$ é o conjunto de todas as cadeias sobre Σ (Veja o Exemplo 2.3). Se $\Sigma = \{0, 1\}$,

$$\Sigma^\star = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, \ldots\}$$

Há apenas uma cadeia vazia, ϵ, com zero símbolos. Com $\Sigma = \{0, 1\}$, temos duas cadeias com um símbolo, 0 e 1. Com dois símbolos existem quatro cadeias, $00, 01, 10, 11$. Com n símbolos, há 2^n cadeias.

Proposição 5.20. *Dado um conjunto finito* Σ*, então* $\Sigma^\star$ *é enumerável.*

Demonstração. Coloque em uma lista a cadeia vazia ϵ, depois todas as cadeias com um símbolo, depois todas com dois símbolos e assim por diante. Esta lista resulta em uma enumeração de $\Sigma^\star$. Isto é possível porque o número de cadeias com n símbolos é finito. De fato, é igual a $|\Sigma|^n$. □

Exemplo 5.45. Se $\Sigma = \{a, e, i, o, u\}$, uma enumeração de $\Sigma^\star$ é:

$$\epsilon, a, e, i, o, u, aa, ae, ai, ao, au, ea, ee, ei, eo, eu, \ldots, aaa, aae, \ldots$$

Então uma função $f : \mathbb{N} \longrightarrow \Sigma^\star$ bijetora pode ser tal que $f(0) = \epsilon$, $f(1) = a$, $f(2) = e$, $f(6) = aa$, $f(30) = aaa$, etc.

Definição 5.42. Uma **linguagem** L sobre um alfabeto Σ é subconjunto de $\Sigma^\star$.

Exemplo 5.46. Se $\Sigma = \{a, e, i, o, u\}$, uma linguagem $L \subset \Sigma^\star$ poderia ser definida da seguinte forma: $L = \{x : x \in \Sigma^\star \text{ e } x \text{ contém a letra } a\}$ Então $iaiau \in L$ mas $ooouu \notin L$.

Sendo Σ o conjunto de todos os caracteres do alfabeto latino, mais espaço e os sinais de pontuação, uma linguagem sobre Σ poderia ser o conjunto de todas os textos da língua portuguesa.

Definição 5.43. Uma **codificação** de uma linguagem $L \subset \Sigma^\star$, Σ finito, é uma função $f : \Sigma^\star \longrightarrow \mathbb{N}$ injetora tal que exista um algoritmo capaz de descobrir se dado $n \in \mathbb{N}$ corresponde ou não a algum elemento $x \in L$ e como identificar tal x.

Mostraremos agora como codificar em números naturais elementos de uma certa linguagem. Antes de mostrar o caso geral, estudaremos um exemplo.

Exemplo 5.47. Codificaremos cada cadeia sobre $\Sigma = \{a, e, i, o, u\}$ usando números binários. Poderíamos usar um número para cada letra:

a	e	i	o	u
0	1	10	11	110

Mas aí o número 10, por exemplo, poderia significar tanto a cadeia *ea* como *i*. E 110 poderia significar *eea*, *oa*, *ei* ou *u*. A codificação não teria inversa; isto é, dado um número, não saberíamos a cadeia que ele codifica. Este problema pode ser resolvido utilizando sempre três símbolos para cada letra:

a	e	i	o	u
000	001	010	011	110

Deste modo não haveria ambiguidades. A cadeia *aue* seria codificada como 000110001. Mas espere: este número é na verdade 110001, pois os zeros à esquerda não contam. Para corrigir isto podemos acrescentar, sempre, o número 1 no início da codificação. Assim, *aue* seria codificada como 1000110001.

Proposição 5.21. *Dado um alfabeto Σ, é possível codificar cada elemento de Σ em um natural de $\lfloor \log_{10} |\Sigma| \rfloor + 1$ dígitos e cada $x \in \Sigma^\star$ em um natural com $[|x| (\lfloor \log_{10} |\Sigma| \rfloor + 1)] + 1$ dígitos.*

Demonstração. Associe cada símbolo de Σ um número natural entre 1 e $|\Sigma|$, preenchendo com zeros à esquerda de tal forma que cada número tenha $\lfloor \log_{10} |\Sigma| \rfloor + 1$ dígitos. Para codificar $s = s_1 s_2 \ldots s_n \in \Sigma^\star$, substitua cada s_i pelo número correspondente e acrescente 1 antes do número resultante. □

Exemplo 5.48. Considere Σ = {a, b, c, ..., z, ' ', . , !, ;, : } ∪ {, }. O símbolo ' ' é o espaço em branco. A associação número/símbolo é

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
t	u	v	w	x	y	z	' '	.	!	;	:	,						
20	21	22	23	24	25	26	27	28	29	30	31	32						

Se o alfabeto tivesse entre 100 e 1000 símbolos, o primeiro símbolo receberia o número 001, o segundo, 002 e assim por diante.

Com esta codificação, podemos mapear qualquer texto de uma linguagem $L \subset \Sigma^\star$ para um número natural. Por exemplo, o texto

muito bem

poderia ser mapeado para o número 1132109201527020513 pela seguinte associação:

$$1\ \overbrace{13}^{m}\ \overbrace{21}^{u}\ \overbrace{09}^{i}\ \overbrace{20}^{t}\ \overbrace{15}^{o}\ \overbrace{27}^{\text{''}}\ \overbrace{02}^{b}\ \overbrace{05}^{e}\ \overbrace{13}^{m}$$

Proposição 5.22. *Há funções de* $\mathbb{N}$ *em* $\mathbb{N}$ *que não podem ser implementadas por um computador.*

Demonstração. Os programas feitos em uma certa linguagem de programação, por exemplo Java, utilizam um certo vocabulário composto pelos símbolos do alfabeto latino, sinais de pontuação e alguns caracteres especiais. Pela Proposição 5.20, pode-se enumerar todos os programas desta linguagem. Isto é, o conjunto de todos os programas em Java é equipotente a $\mathbb{N}$. Mas o conjunto de todas as funções de $\mathbb{N}$ em $\mathbb{N}$ é equipotente a $\mathbb{R}$ (veja Exercício 5.61). Então há funções $f : \mathbb{N} \longrightarrow \mathbb{N}$ que não podem ser implementadas pela linguagem Java. Como esta linguagem pode implementar qualquer algoritmo,[5] há problemas que não podem ser solucionados por nenhum algoritmo. □

Exemplo 5.49. O conjunto de todas as fórmulas de uma linguagem da Lógica de Primeira Ordem é enumerável. Mostraremos uma codificação de uma maneira diferente da apresentada acima.

Considere uma linguagem $\mathcal{L}$ da lógica de primeira ordem associada a um vocabulário $\mathcal{V} = (\Sigma, \Delta, \Psi)$ no qual Σ é um conjunto de símbolos de predicado, Δ é um conjunto de símbolos de função e Ψ é um conjunto de símbolos de constante. Todos estes conjuntos devem ser finitos, por definição.

A linguagem $\mathcal{L}$, além dos símbolos $\Sigma \cup \Delta \cup \Psi$, utiliza os símbolos

$$\forall, \exists, (,), \neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$$

mais a vírgula "," e x_i para todo $i \in \mathbb{N}$.

Associaremos cada um destes símbolos a um número de $\mathbb{N}$:

(a) a cada elemento de $S = \Sigma \cup \Delta \cup \Psi$ associamos um número da forma $1\ \overbrace{00...0}^{k}\ 1$ no qual k é o número de zeros entre os dois 1´s. Cada símbolo de S é associado a um número k entre 1 e $|S|$. Por exemplo, se $S = \{P, I, +, c_1, c_2\}$, então os símbolos P, I, $+$, c_1 e c_2 são associados, respectivamente, aos números 101, 1001, 10001, 100001, 1000001.

(b) $\forall, \exists, (,), \neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$ e "," são associados aos números 202, 2002, 20002, 200002, 2000002, ...

(c) x_i é associado ao número $3\ \overbrace{00...0}^{i}\ 3$, no qual i é o número de zeros e o índice de x_i. Assim x_1 e x_5, por exemplo, são associados aos números 303 e 3000003, respectivamente.

[5] Assuma isto. Há alguns detalhes técnicos que não serão discutidos a este respeito.

Note que nem todos os números estão associados a fórmulas. Por exemplo,
202303556
não está associado a uma fórmula pois 556 não está associado a nenhuma parte de nenhuma linguagem $\mathcal{L}$.

É fácil provar que esta associação define uma função injetora entre o conjunto de todas as fórmulas e os números naturais. Eliminando-se os números que não estão associados a nenhuma fórmula, obtemos uma função bijetora entre o conjunto de todas as fórmulas e os naturais restantes. Mas há, por sua vez, uma bijeção entre estes e $\mathbb{N}$. Logo o conjunto de todas as fórmulas é enumerável.

Proposição 5.23. *Não há fórmulas da LPO suficientes para definir todos os números reais.*

Demonstração. Pode-se definir números reais utilizando-se fórmulas da LPO com uma variável livre como em

$$A(y) =_{def} \exists x\,(x \,.\, x = y)$$

Esta fórmula define o número real $\sqrt{2}$, se utilizarmos uma linguagem e estrutura apropriados. Isto é, o único número y tal que $A(y)$ é verdade no modelo dos reais é $y = \sqrt{2}$.

Como o conjunto das fórmulas da LPO é enumerável e o conjunto $\mathbb{R}$ não o é, não há fórmulas suficientes para definir todos os números reais. □

Definição 5.44. A cada conjunto A está associado um outro conjunto $|A|$ chamado de **cardinalidade** de A de tal forma que $|A| = |B|$ se e somente se $A \sim B$. Também usamos card A para representar $|A|$.

Se $A \neq \emptyset$ for um conjunto finito com k elementos, $|A| = k$ Se A for o conjunto vazio, a sua cardinalidade é 0. Se A for infinito, $|A|$ é um dos conjuntos $\aleph_0, \aleph_1, \aleph_2, \ldots$. Em particular, $|\mathbb{N}| = \aleph_0$. E valem as desigualdades: $\aleph_i < \aleph_{i+1}$ para todo $i \in \mathbb{N}$. Os conjuntos cardinais infinitos são chamados de números **transfinitos**. A cardinalidade de $\mathbb{R}$ é chamada de c, que é igual à cardinalidade de $2^{\mathbb{N}}$. A famosa hipótese do contínuo diz que $c = \aleph_1$. Tanto esta hipótese como a negação dela são consistentes com os axiomas de ZFC (veja Seção 5.9).

Definição 5.45. Dados os conjuntos A e B, escreveremos $|A| \leqslant |B|$ se houver uma função $f : A \longrightarrow B$ injetora. Escrevemos $|A| < |B|$ se $|A| \leqslant |B|$ mas A não é equipotente a B. Isto é, escrevemos $|A| < |B|$ se houver uma função injetora $f : A \longrightarrow B$ mas não houver nenhuma função injetora $g : B \longrightarrow A$.

Note que se há uma função injetora $f : A \longrightarrow B$, com A e B finitos, necessariamente teremos $|A| \leqslant |B|$. Isto acontece porque dois elementos $x, y \in A$ necessariamente produzirão duas imagens distintas $f(x), f(y)$ em B. Então n elementos de A produzirão n elementos distintos em B pela aplicação de f. Mas podem "sobrar" elementos de B, elementos $z \in B$ para os quais não há um $x \in A$ tal que $f(x) = z$.

Aplicando o raciocínio para conjuntos infinitos, se há uma função $f : A \longrightarrow B$ injetora, de certa forma B é pelo menos tão "grande" quanto A. De fato, definimos que, neste caso, card $A \leqslant$ card B.

Exemplo 5.50. Usando a notação definida acima, podemos afirmar que:

(a) $|\mathbb{N}| \leqslant |\mathbb{R}|$ e $|\mathbb{N}| < |\mathbb{R}|$

(b) $|\mathbb{N}| \leqslant |\mathbb{Q}|$ e $|\mathbb{Q}| \leqslant |\mathbb{N}|$

(c) $|\mathbb{Z}| \leqslant |\mathbb{Q}|$ e $|\mathbb{Q}| \leqslant |\mathbb{Z}|$

(d) $|(0,1)| \leqslant |\mathbb{R}|$ e $|\mathbb{N}| \leqslant |(0,1)|$, no qual $|(0,1)|$ é a cardinalidade do intervalo $(0,1)$

(e) $|\mathbb{Q}| < |\mathbb{R}|$, card $2^{\mathbb{N}} <$ card $\mathbb{R}$

(f) $|S| < |\mathbb{R}|$, no qual S é o conjunto de todos os possíveis programas de um computador.

Teorema 5.1. *(Cantor-Schröder-Bernstein)*
Se $|A| \leqslant |B|$ e $|B| \leqslant |A|$ então $|A| = |B|$. Isto é, se houver funções injetoras $f : A \longrightarrow B$ e $g : B \longrightarrow A$, então há uma função bijetora $h : A \longrightarrow B$.

Exemplo 5.51. Há uma função injetora $f : \mathbb{N} \longrightarrow \mathbb{Q}$, a saber, $f(n) = n$. E uma função injetora $g : \mathbb{Q} \longrightarrow \mathbb{N}$, a saber, $g(0) = 0$ e $g(a/b) = 2^a 3^b$ para $a \neq 0$ e $b \neq 0$, no qual a e b não têm divisores em comum (como 15 e 6, que são ambos divisíveis por 3). Então $\mathbb{N} \sim \mathbb{Q}$ pelo Teorema 5.1.

Proposição 5.24. *Seja A um conjunto. Então $|A| < |\mathcal{P}(A)|$; isto é a cardinalidade de um conjunto é menor do que o do seu conjunto das partes.*

Exemplo 5.52. Seja $A = \{0, 1, 2\}$. Então

$$\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$$

A cardinalidade de A, $|A|$, é 3. E a de $\mathcal{P}(A)$ é 8. E $3 < 8$.

Pelo Exercício 5.62, $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$. Como $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ pela Proposição 5.24, temos $|\mathbb{N}| < |\mathbb{R}|$. Isto é, $\mathbb{N}$ não é equipotente a $\mathbb{R}$.

Exercícios

5.45. Prove se A é um conjunto infinito e $x_0 \in A$, então $A - \{x_0\}$ é infinito.

5.46. Prove que são finitos os seguintes conjuntos:

(a) $\emptyset$

(b) $\{1\}$

(c) $\{0, 1, 2, \ldots k\}$, utilize indução e o exercício 5.45.

5.47. Prove a Proposição 5.7, que a relação $\sim$ é uma relação de equivalência.

5.48. Prove se B é um conjunto infinito e $B \subset A$, então A é infinito.

5.49. Prove se A é um conjunto infinito e existe $f : A \longrightarrow B$ bijetora, então B é infinito.

5.50. Prove que os seguintes conjuntos são equipotentes a $\mathbb{N}$.

(a) O conjunto dos números ímpares.

(b) O conjunto dos números divisíveis por 3.

(c) O conjunto das potências de 2.

(d) O conjunto dos números divisíveis por 2 e 7.

(e) O conjunto das retas $y = ax + b$ nas quais $a, b \in \mathbb{N}$.

(f) A^2, dado que $A = \{0, 1, 2, \ldots 20\}$.

(g) $A \times \mathbb{N}$, dado que $A = \{0, 1\}$.

(h) $\{a + bi : a, b \in \mathbb{N} \text{ e } i = \sqrt{-1}\}$

(i) $A \cup B \cup C$, onde A, B e C são enumeráveis.

(j) $A_0 \cup A_1 \cup \ldots A_{n-1}$, onde A_i, $0 \leqslant i < n$, é enumerável.

5.51. Suponha que o Universo físico possui infinitos planetas com vida. Então podemos afirmar que em um destes planetas há um saci-pererê?

5.52. Considere um cubo aberto no plano xyz cujas dimensões sejam $(0, 1) \times (0, 1) \times (0, 1)$. Podemos afirmar que há uma correspondência um a um entre os pontos deste cubo e o segmento de reta $(0, 1)$?

5.53. Sobre alfabetos e linguagem, faça:

(a) defina um alfabeto Σ qualquer com pelo menos três símbolos;

(b) crie duas linguagem L_1 e L_2 diferentes sobre Σ;

(c) dê pelo menos seis elementos de $\Sigma^\star$;

(d) calcule $L_1 \cap L_2$.

5.54. Dado o alfabeto $\Delta = \{0, 1, 2, 3\}$, faça:

(a) dê pelo menos seis elementos de $\Delta^\star$;

(b) O conjunto $\{0^n 13^n : n \in \mathbb{N}\}$ é uma linguagem sobre Δ? 0^n quer dizer n símbolos 0´s;

(c) descreva formalmente a linguagem L sobre Δ tal que todo $x \in L$ começa com 0;

(d) quantos elementos tem o conjunto $\{x \in \Delta^\star : |x| = 4\}$?

5.55. Faça uma codificação para o cálculo proposicional. Os símbolos permitidos são:

$$\{(,), \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\} \cup \{V_i : i \in \mathbb{N}\}$$

5.56. A linguagem do Cálculo Proposicional utiliza os símbolos $(,), \neg, \vee$ e V_i para todo $i \in \mathbb{N}$. Uma fórmula do CP é definido como

(a) uma variável V_i é uma fórmula;

(b) $\neg A$ e $(A \vee B)$ são fórmulas se A e B são fórmulas;

(c) fórmulas são descritas apenas pelos itens (a) e (b).

Então são fórmulas: V_0, V_3, $(V_0 \vee V_3)$, $\neg(V_0 \vee V_3)$, $\neg V_0$, $\neg V_3$, $(\neg V_0 \vee \neg V_3)$ e $\neg\neg V_0$.

Considere uma codificação para o CP tal que, se $\sharp A$ é o número que representa A, então as representações das fórmulas são:

Fórmula	Código
$\neg A$	$2^{\sharp A}$
$(A \vee B)$	$3^{\sharp A}5^{\sharp B}$
V_i	7^i

Faça então:

(a) a codificação de V_0, $\neg V_0$, $(\neg V_0 \vee V_3)$ e $\neg(V_4 \vee \neg(\neg V_0 \vee V_3))$;

(b) a prova de que, se $A \neq B$, então $\sharp A \neq \sharp B$ (ou pelo menos explique intuitivamente porque os códigos devem ser diferentes se as fórmulas são diferentes);

(c) a prova de que as fórmulas do CP são enumeráveis.

5.57. Faça uma codificação semelhante à do exercício anterior para a Lógica de Primeira Ordem.

5.58. Prove que o conjunto de todos os quadros quadrados com pinturas são enumeráveis assumindo que:

1. o menor quadro possui 1cm ×1cm;
2. os tamanhos dos quadros diferem em pelo menos 0.1cm (1, 1.1, 1.2, 1.3, . . ., 100, 100.1, . . .);
3. o olho humano consegue diferenciar no máximo 10^{10} cores (deve ser menos!) em superfícies de no máximo 0.00001×0.00001 centímetros (na realidade estes números devem ser maiores).

5.59. Assumindo as limitações de quadros dadas pelo exercício anterior, estime o número de quadros quadrados de pintura até 100cm ×100cm.

5.60. Faça uma codificação para grafos $G = (V, E)$ nos quais $V \subset \mathbb{N}$.

5.61. Seja S o conjunto de todas as funções $f : \mathbb{N} \longrightarrow \mathbb{N}$. Prove que $S \sim \mathbb{R}$. Dica: faça uma função injetora entre S e $\mathbb{R}$ e outra função injetora entre $\mathbb{R}$ e S. A primeira mapeia cada função f de S em um número $0.\overline{f(0)}2\overline{f(1)}2\overline{f(2)}2\ldots \in (0, 1)$ tal que $\overline{f(n)}$ é o número $f(n)$ em binário. Por exemplo, se $f(n) = n$ o número seria $0.0212102\ldots$ A função injetora entre $\mathbb{R}$ e S toma $n.d_1d_2d_3\ldots$ e mapeia para $f : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $f(0) = n$, $f(1) = d_1$, etc.

5.62. Prove que o conjunto das partes de $\mathbb{N}$ é equipotente a $\mathbb{R}$; isto e, $2^{\mathbb{N}} \sim \mathbb{R}$. Dica: veja a resolução do exercício anterior. Associe a cada subconjunto de $\mathbb{N}$ a sua função característica ...

Capítulo 6

Álgebra

6.1 Grupos

Uma estrutura $\langle G, \mathbf{.} \rangle$ é um **grupo** se $G \neq \emptyset$ e $\mathbf{.}$ é uma operação binária definida como

$$\mathbf{.} : G \times G \longrightarrow G$$

e tal que as seguinte propriedades são satisfeitas:
, para quaisquer elementos $a, b, c \in G$, temos:

associativa para quaisquer $a, b, c \in G$ temos $a \mathbf{.} (b \mathbf{.} c) = (a \mathbf{.} b) \mathbf{.} c$;

identidade existe $e \in G$ tal que $a \mathbf{.} e = e \mathbf{.} a = a$ para todo $ainG$;

inverso para todo $a \in G$ existe $x \in G$ tal que $a \mathbf{.} x = x \mathbf{.} a = e$.

Então todo grupo possui um elemento chamado de **identidade** ou **elemento neutro** que é usualmente denotado por e. Este é um elemento de G que sempre que operação binária $\mathbf{.}$ é aplicada a ele juntamente com outro elemento a, resulta no próprio a. Além disso, em um grupo, cada elemento a possui um elemento chamado de **inverso** de a. O inverso de a é o elemento $x \in G$ tal que $a \mathbf{.} x = x \mathbf{.} a = e$, onde e é o elemento de identidade. Tipicamente detonamos o elemento inverso x por a^{-1} para explicitar o fato deste ser o inverso de a. Mas veja que a^{-1} é uma notação, este elemento possui um símbolo associado a ele que não é a^{-1}, é x.

O símbolo da operação binária de um grupo não precisa ser "$\mathbf{.}$". De fato, o símbolo em si não importa. Então podemos usar outros símbolos para a operação, como $+$, $\star$, $\oplus$, etc.

Freqüentemente escrevemos "G é um grupo", quando a operação binária utilizada está implícita. O mais correto seria afirmar "$\langle G, \mathbf{.} \rangle$" é um grupo, sempre explicitando a operação considerada. No entanto, usaremos as duas notações neste livro, por conveniência. E quando não houver ambigüidade quanto à operação utilizada, escrevemos ab no lugar de $a \mathbf{.} b$.

Definição 6.1. Um grupo $\langle G, \mathbf{.} \rangle$ é chamado de **abeliano** [1] se a operação $\mathbf{.}$ é comutativa; isto é, para quaisquer $a, b \in G$, temos $a \mathbf{.} b = b \mathbf{.} a$.

Exemplo 6.1. A estrutura $\langle \mathbb{Z}, + \rangle$ é um grupo abeliano, onde + é a operação de soma usual entre inteiros. Vamos conferir. Para todo $a, b, c \in \mathbb{Z}$,

(a) $a + (b + c) = (a + b) + c$, pois a soma de inteiros é associativa;

(b) o elemento identidade é 0. De fato, $0 + a = a + 0 = a$ para todo $a \in \mathbb{Z}$;

(c) o elemento inverso de $b \in \mathbb{Z}$ é $-b \in \mathbb{Z}$: $b + (-b) = (-b) + b = 0$;

(d) $a + b = b + a$.

Exemplo 6.2. A estrutura $\langle \mathbb{Q}, + \rangle$ é um grupo abeliano, onde + é a operação de soma usual entre racionais. Portanto, a operação de soma é associativa e comutativa. Todo elemento de $\mathbb{Q}$ pode ser escrito como $\frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$. A identidade é 0 e o inverso de $\frac{a}{b}$ é $\frac{-a}{b}$.

Exemplo 6.3. A estrutura $\langle \mathbb{N}, + \rangle$ não é um grupo. Há um elemento identidade 0 mas não há elemento inverso para todo $a > 0$.

Definição 6.2. Denotamos por $M_n(S)$ o conjunto de todas as matrizes $n \times n$ com elementos em S. Assim, $M_2(\mathbb{R})$ é o conjunto de todas as matrizes 2×2 cujos elementos são reais.

Exemplo 6.4. O conjunto $M_2(\mathbb{R})$ com a operação + entre matrizes é um grupo abeliano. Vejamos: para toda matriz A, B e C deste conjunto,

(a) $A + (B + C) = (A + B) + C$, pois a soma de matrizes é associativa;

(b) o elemento identidade é

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(c) para uma matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

o elemento inverso é

$$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

(d) $A + B = B + A$.

Exemplo 6.5. $M_2(\mathbb{R})$ com a operação $\mathbf{.}$ de multiplicação entre matrizes não é um grupo. Vejamos: para toda matriz A, B e C deste conjunto,

(a) $A \mathbf{.} (B \mathbf{.} C) = (A \mathbf{.} B) \mathbf{.} C$;

[1] Em homenagem a Abel, matemático norueguês.

(b) o elemento identidade é a matriz identidade

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(c) para uma matriz A, o inverso é a matriz A^{-1}. Mas nem toda matriz pode ser invertida. Então o conjunto de todas as matrizes 2×2 não formam um grupo.

Exemplo 6.6. O conjunto de todas as matrizes 2×2 invertíveis com elementos em $\mathbb{R}$ e com a operação $\cdot$ de multiplicação entre matrizes é um grupo. A multiplicação entre matrizes é associativa, há um elemento identidade I (matriz identidade) e toda matriz possui inverso. Este grupo não é abeliano, pois no caso geral, $A \cdot B \neq B \cdot A$.

Exemplo 6.7. Seja G_n o conjunto de todos os números binários que possuem exatamente n bits. O conjunto G_n forma com a operação "ou exclusivo bit-a-bit" um grupo abeliano. A operação "ou exclusivo bit-a bit" é um ou exclusivo realizado em cada bit. Por exemplo, $1100 \oplus 1010 = 0110$. Não é difícil ver que o inverso de um elemento é ele mesmo.

Exemplo 6.8. O conjunto $\mathbb{Z}_n$ com adição módulo n forma um grupo abeliano. A prova é deixada como exercício.

Exemplo 6.9. Considere o conjunto $G = \{I, A, B, C\}$ tal que cada elemento representa transformações em um retângulo não quadrado. I é a transformação identidade, A é a reflexão sobre a linha média entre os dois maiores lados do retângulo, B é a reflexão sobre a linha média entre os dois menores lados e C é a rotação por 180°. A operação $\star$ é a composição de transformações: AB por exemplo é a transformação A seguida da transformação B. A operação $\star$ possui a seguinte tabela de composição:

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

A estrutura $\langle G, \star \rangle$ é um grupo. Confira.

Definição 6.3. Um **monóide** é uma estrutura $\langle M, \cdot \rangle$ tal que a operação $\cdot$ é associativa e existe um elemento identidade em M.

Definição 6.4. Um **semigrupo** é uma estrutura $\langle S, \cdot \rangle$ tal que a operação $\cdot$ é associativa.

Exemplo 6.10. Seja Σ um conjunto de símbolos quaisquer chamado de alfabeto, $\Sigma \neq \emptyset$. O conjunto $\Sigma^\star$ é composto por concatenações de símbolos de Σ; isto é, símbolos de Σ colocados lado a lado. Cada elemento de $\Sigma^\star$ é chamado de *cadeia* (*string*). O conjunto $\Sigma^\star$ é definido indutivamente como

- $\varepsilon \in \Sigma^\star$, onde ε é a cadeia vazia;
- se $a \in \Sigma$, então $a \in \Sigma^\star$;
- se $s, t \in \Sigma^\star$, $s \,.\, t \in \Sigma^\star$, no qual $s \,.\, t$ é uma cadeia que é a concatenação dos símbolos de s com os símbolos de t, que é denotado por st. Então $s \,.\, t = st$. Por exemplo, se $s = 101$ e $t = 00$, então $st = 10100$ e $ts = 00101$.

Se $\Sigma = \{0, 1\}$, então $\Sigma^\star = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$.

A estrutura $\langle \Sigma^\star, . \rangle$, onde $.$ é a operação de concatenação, é um monóide mas não é um grupo. A prova é deixada como exercício.

Definição 6.5. A **ordem** de um grupo $\langle G, . \rangle$ é o número de elementos de G, isto é, $|G|$.

Definição 6.6. Se usamos $.$ como símbolo de operação de um grupo, usualmente usamos 1 para o elemento identidade e a^{-1} para o inverso de a. Usamos a^n para representar

$$\overbrace{a \,.\, a \,.\, a \ldots a}^{n}$$

se $n \in \mathbb{N}^\star$. Se $n = 0$, a^n denota 1 e, se $n \in \mathbb{Z}, n < 0$, a^n denota $(a^{-n})^{-1}$. Chamamos a operação $.$ de **produto**.

Se usamos + como símbolo para a operação de um grupo, usualmente usamos 0 para o elemento identidade e $-a$ para o inverso de a. Se $n \in \mathbb{N}^\star$, usamos na para representar

$$\overbrace{a + a + \ldots a}^{n}$$

Se $n = 0$, $na = 0$ e se $n \in \mathbb{Z}, n < 0$, na denota $-((-n)a)$. O termo $a - b$ é utilizado para $a + (-b)$. Chamamos a operação + de **soma**.

Veremos agora algumas propriedades de grupos.

Proposição 6.1. *O elemento identidade é único.*

Demonstração. Seja $\langle G, . \rangle$ um grupo. Suponha que existam dois elementos de identidade e_1 e e_2 (deve haver pelo menos um pela definição de grupo). Então

$$e_1 \,.\, e_2 = e_1 \text{ pois } e_2 \text{ é elemento identidade, e}$$

$$e_1 \,.\, e_2 = e_2 \text{ pois } e_1 \text{ é elemento identidade.}$$

Logo $e_1 = e_2$.

□

Proposição 6.2. *O elemento inverso de cada elemento é único.*

Demonstração. Seja $\langle G, . \rangle$ um grupo. Seja $a \in G$ e suponha que existam $b, c \in G$ tais que ambos sejam inversos de a. Então pela definição de inverso, temos

$$a \,.\, b = b \,.\, a = e = c \,.\, a = a \,.\, c$$

onde e é a identidade. Multiplicando ambos os lados da equação

$$a \,.\, b = a \,.\, c$$

por b temos

$$\begin{aligned} b \,.\, (a \,.\, b) &= b \,.\, (a \,.\, c) \\ (b \,.\, a) \,.\, b &= (b \,.\, a) \,.\, c \\ e \,.\, b &= e \,.\, c \\ b &= c \end{aligned}$$

□

Proposição 6.3. *O inverso de $a \,.\, b$ é $b^{-1} \,.\, a^{-1}$.*

Demonstração. Sendo e o elemento identidade do grupo, temos

$$\begin{aligned} (a \,.\, b) \,.\, (b^{-1} \,.\, a^{-1}) &= a \,.\, (b \,.\, (b^{-1} \,.\, a^{-1})) \\ &= a \,.\, ((b \,.\, b^{-1}) \,.\, a^{-1}) \\ &= a \,.\, (e \,.\, a^{-1}) \\ &= a \,.\, a^{-1} \\ &= e \end{aligned}$$

Logo $b^{-1} \,.\, a^{-1}$ é o inverso de $a \,.\, b$.

□

Exemplo 6.11. Considere o conjunto $G = \{e, x, y, z\}$ e a operação $\star$ definida pela seguinte tabela:

$\star$	e	x	y	z
e	e	x	y	z
x	x	x	e	e
y	y	e	y	e
z	z	e	e	z

A estrutura $\langle G, \star \rangle$ não é um grupo pois y e z são ambos inversos de x:

$$x \star y = y \star x = e, x \star z = z \star x = e$$

Então o inverso não é único. Não pode ser um grupo.

Definição 6.7. Seja $\langle G, \mathbf{.} \rangle$ um grupo e $H \subset G$. Se $\langle H, \mathbf{.} \rangle$ for um grupo, então será chamado de **subgrupo** de G.[2]

Proposição 6.4. *Um subconjunto H de G é um grupo se:*

(a) $e \in H$, onde e é a identidade de G;

(b) para todo $a \in H$, $a^{-1} \in H$;

(c) para todo $a, b \in H$, $a \mathbf{.} b \in H$. Isto é, H é fechado sobre a operação "$\mathbf{.}$".

Exemplo 6.12. $H = \langle \{0, 1, 2\}, + \rangle$ não é um subgrupo de $G = \langle \mathbb{Z}, + \rangle$ pois $1 + 2 = 3$ e $3 \notin \{0, 1, 2\}$. Além disto, os inversos aditivos de 1 e 2 não pertencem ao conjunto $\{0, 1, 2\}$. A estrutura $\langle \{0, -1, 1\}, + \rangle$, embora tenha o inverso de todos os elementos pertencentes ao conjunto, também não é subgrupo de G pois $1 + 1 = 2 \notin \{0, -1, 1\}$. Note que a operação $+$ em ambos os casos é herdada de G e é a soma entre inteiros.

Definição 6.8. O conjunto $\mathbb{Z}_n$ utiliza a soma módulo n. A maneira mais fácil de entender isto é considerando que $\mathbb{Z}_n$ é composto por $\overline{0}, \overline{1}, \ldots \overline{n-1}$ e que o próximo número depois de $\overline{n-1}$ é $\overline{0}$. Forma-se um ciclo. Assim, se uma soma de dois elementos de $\mathbb{Z}_n$ for dar $\overline{n}$, na verdade o resultado é $\overline{0}$. Se a soma resultar em $\overline{n+1}$, o resultado é $\overline{1}$ e assim por diante.

Assim, se $\overline{a}, \overline{b} \in \mathbb{Z}_n$, $\overline{a} + \overline{b} = \overline{k}$ se $a + b \equiv k \pmod{n}$. Por exemplo, em $\mathbb{Z}_5$, $\overline{2} + \overline{3} = \overline{0}$, pois $2 + 3 \equiv 0 \pmod{5}$; isto é, 5 é divisível por 5. Vejamos outras somas em $\mathbb{Z}_5$:

$$\begin{aligned} \overline{2} + \overline{2} &= \overline{4} \\ \overline{4} + \overline{4} &= \overline{8} = \overline{5+3} = \overline{5} + \overline{3} = \overline{0} + \overline{3} = \overline{3} \\ \overline{4} + \overline{3} &= \overline{7} = \overline{5+2} = \overline{5} + \overline{2} = \overline{0} + \overline{2} = \overline{2} \end{aligned}$$

Lembre-se de que $\overline{k}$ em $\mathbb{Z}_5$ é o conjunto formado por todos os inteiros (pertencentes a $\mathbb{Z}$) cujo resto da divisão são iguais quando divididos por 5. Assim,

$$\overline{2} = \{k \in \mathbb{Z} : k \text{ dividido por 5 deixa resto 2}\}$$

Exemplo 6.13. $G = \langle Z_6, + \rangle$, no qual $+$ é a soma módulo 6, é um grupo. E são subgrupos de G:

1. $H = \{\overline{0}\}$
2. $H = \{\overline{0}, \overline{2}, \overline{4}\}$. Vejamos: $\overline{0} + \overline{2} = \overline{2} \in H$, $\overline{0} + \overline{4} = \overline{4} \in H$, $\overline{2} + \overline{4} = \overline{0} \in H$, $\overline{0} + \overline{0} = \overline{0}$ ($\overline{0} = -\overline{0}$, usamos $-$ para a operação inversa), $\overline{2} + \overline{4} = \overline{0}$ ($\overline{2}$ e $\overline{4}$ são inversos um do outro). Como este grupo é comutativo, temos $\overline{2} + \overline{0} = \overline{2} \in H$ e assim por diante;
3. $H = \{\overline{0}, \overline{3}\}$. Vejamos: $\overline{0} + \overline{3} = \overline{3} \in H$, $\overline{3} + \overline{0} = \overline{3} \in H$, $\overline{3} + \overline{3} = \overline{0} \in H$. Todos os elementos são inversos de si mesmos;

[2] Usualmente diz-se "G é um grupo" quando o correto seria "$\langle G, \mathbf{.} \rangle$ é um grupo".

4. $H = G$ é um subgrupo. Todo grupo é subgrupo de si mesmo.

Note que aqui colocamos apenas os subconjuntos como se fossem grupos. A operação utilizada está implícita — é o + módulo 6 herdado de G.

Definição 6.9. Seja $\langle G, \mathbf{.} \rangle$ um grupo. Um elemento $g \in G$ é chamado de **gerador** de G se e somente se todo elemento $a \in G$ pode ser expresso como g^n ou g^{-n}, no qual

$$\begin{aligned} g^0 &= e \\ g^n &= \overbrace{g \mathbf{.} g \mathbf{.} g \mathbf{.} \cdots g}^{n} \\ g^{-n} &= (g^{-1})^n = \overbrace{g^{-1} \mathbf{.} g^{-1} \mathbf{.} g^{-1} \mathbf{.} \cdots g^{-1}}^{n} \end{aligned}$$

O elemento e é a identidade.

Um grupo é chamado de **cíclico** se contiver um elemento gerador.

Exemplo 6.14. O grupo $\mathbb{Z}_n$ é cíclico e gerado por $\overline{1}$. Por exemplo, considere $\mathbb{Z}_3$. Então $\overline{1} = \overline{1}, \overline{2} = \overline{1} + \overline{1}, \overline{0} = \overline{1} + \overline{1} + \overline{1}$.

Exemplo 6.15. O grupo $\langle \mathbb{Z}, + \rangle$ é cíclico. Tanto 1 como -1 o geram.

Definição 6.10. Seja $\langle G, \mathbf{.} \rangle$ um grupo e $H \subset G$. O **subgrupo gerado** por H consiste da aplicação da operação $\mathbf{.}$ nos elementos de H e seus inversos. Então o subgrupo J gerado por H é definido indutivamente como

- $x \in J$ se $x \in H$;
- $x^{-1} \in J$ se $x \in J$;
- $x \mathbf{.} y \in J$ se $x, y \in J$.

Note que H é um subconjunto de G, não um subgrupo.

Exemplo 6.16. O subconjunto $\{-2, 3\}$ de $\mathbb{Z}$ pode gerar todos os elementos do grupo $\langle \mathbb{Z}, + \rangle$. Vejamos alguns elementos de J, o grupo gerado por $\{-2, 3\}$.

$$\begin{aligned} -6 &\in J \text{ pois } -6 = -2 + ((-2) + (-2)) \\ 6 &\in J \text{ pois } 6 = 3 + 3 \\ 0 &\in J \text{ pois } 0 = 6 + (-6) \\ 1 &\in J \text{ pois } 1 = (-2) + 3 \\ -1 &\in J \text{ pois } -1 = 2 + (-3) \end{aligned}$$

Como $1, -1 \in J$, todo elemento de $\mathbb{Z}$ pode ser gerado a partir de $\{-2, 3\}$.

Exemplo 6.17. O subconjunto de $\mathbb{Z}$ formado pelos pares não gera $\mathbb{Z}$. Soma de pares não geram números ímpares.

Definição 6.11. Um **homomorfismo** f entre grupos $\langle G, \mathbf{.} \rangle$ e $\langle H, + \rangle$ é uma função $f : G \longrightarrow H$ tal que

$$f(a \mathbf{.} b) = f(a) + f(b)$$

Definição 6.12. Um **isomorfismo** f entre grupos $\langle G, \mathbf{.} \rangle$ e $\langle H, + \rangle$ é uma função **bijetora** $f : G \longrightarrow H$ tal que

$$f(a \mathbf{.} b) = f(a) + f(b)$$

Se dois grupos são isomorfos, eles são iguais a menos de nomes de elementos e da operação.

Proposição 6.5. *Seja $f : G \longrightarrow H$ um isomorfismo entre os grupos $\langle G, \mathbf{.} \rangle$ e $\langle H, + \rangle$. Considerando que os elementos de identidade são 1 e 0, temos que $f(1) = 0$.*

Demonstração. Seja y um elemento de H. Como f é bijetora, existe $a \in G$ tal que $f(a) = y$. Então

$$\begin{aligned} f(1) + y &= f(1) + f(a) \\ &= f(1 + a) \\ &= f(a) \\ &= y \end{aligned}$$

Analogamente, $y + f(1) = y$, onde y é um elemento qualquer de H. Logo $f(1)$ é uma identidade em H e, como a identidade é única, $0 = f(1)$. □

Exercícios

6.1. Prove que o $M_3(\mathbb{R})$ com a operação **.** de multiplicação de matrizes é um monóide.

6.2. Prove que não são grupos:

(a) $M_2(\mathbb{N})$ com a operação + de soma entre matrizes;

(b) $\langle \mathbb{Z}, - \rangle$. De fato, prove que esta estrutura não é um monóide ou semigrupo;

(c) $M_2(\mathbb{Z})$ com a operação **.** de multiplicação entre matrizes;

(d) $\langle \mathbb{Q}, \mathbf{.} \rangle$, onde **.** é a multiplicação.

6.3. Verifique que o operador definido pela tabela do exemplo 6.11 não é associativo.

6.4. Prove que $\langle M, \mathbf{.} \rangle$ é um grupo, no qual $M = \{A \in M_2(\mathbb{R}) : |\det A| = 1\}$. Este grupo é abeliano? Usamos $|x|$ para módulo de x e $\det A$ para determinante de A. A operação $\mathbf{.}$ é a multiplicação de matrizes.

6.5. Modifique a tabela do exemplo 6.11 de tal forma que $\langle G, \star \rangle$ se transforme em um grupo.

6.6. Considere o conjunto $G = \{x, y, z\}$. Faça tabelas para o operador $\mathbf{.}$ tal que $\langle G, \mathbf{.} \rangle$:

(a) seja um grupo;

(b) não seja um grupo

6.7. Calcule:

(a) $\overline{0} + \overline{2}$, $\overline{1} + \overline{4}$, $\overline{2} + \overline{3}$ em $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ e $\mathbb{Z}_5$;

(b) $2\overline{2}$, $3\overline{2}$, $4\overline{2}$ e $5\overline{2}$ em $\mathbb{Z}_3$ e $\mathbb{Z}_4$ (lembre-se de que $2\overline{2} = \overline{2} + \overline{2}$);

(c) $\overline{n/2} + \overline{n/2}$ em $\mathbb{Z}_n$, n par;

(d) $\overline{\lceil n/2 \rceil} + \overline{\lfloor n/2 \rfloor}$ em $\mathbb{Z}_n$, n ímpar.

6.8. Prove que

(a) $(a^{-1})^{-1} = a$

(b) se $a \mathbf{.} b = a \mathbf{.} c$, então $b = c$;

(c) se $b \mathbf{.} a = c \mathbf{.} a$, então $b = c$;

(d) em um grupo G, a equação $a \mathbf{.} x = b$ tem uma única solução em x.

6.9. Prove que a estrutura do exemplo 6.10 é um monóide mas não é um grupo.

6.10. Pergunta-se:

(a) é $\overline{3}$ um gerador para $\mathbb{Z}_5$? E $\overline{2}$?

(b) é $\overline{5}$ um gerador para $\mathbb{Z}_7$?

(c) é $\{\overline{1}, \overline{3}\}$ um subconjunto gerador para $\mathbb{Z}_5$? E para $\mathbb{Z}_7$?

6.11. Prove que, se $f : G \longrightarrow H$ é um isomorfismo entre os grupos G e H, então $f(a)^{-1} = f(a^{-1})$.

6.12. Prove que $\mathbb{Z}_2$ com a operação de soma módulo 2 é isomorfo ao grupo com elementos $\{e, x\}$ cuja operação $\star$ é dada pela tabela

$\star$	e	x
e	e	x
x	x	e

6.13. Prove que $\langle \mathbb{R}_*^+, . \rangle$ é isomorfo a $\langle \mathbb{R}, + \rangle$.

6.14. Encontre dois subgrupos de $\langle \mathbb{Z}, + \rangle$.

6.15. Prove que $\{0\}$ é um subgrupo de $\langle G, + \rangle$. Lembre-se de que usamos 0 para a identidade quando o símbolo para a operação do grupo for $+$.

6.16. Encontre um subconjunto infinito que gere:

(a) $\langle \mathbb{Z}, + \rangle$ e que seja diferente de $\mathbb{Z}$;

(b) $\langle \mathbb{Q}, + \rangle$ e que seja diferente de $\mathbb{Q}$.

Apêndice A

Fórmulas Importantes

Fórmulas com logaritmos

Nas fórmulas abaixo, e é a base do logaritmo natural.

$$\log ab = \log a + \log b$$

$$\log_a b = \frac{\log_c b}{\log_c a}$$

$$a^b = e^{b \ln a}$$

$$\log_b a^n = n \log_b a$$

$$a^{\log b} = b^{\log a}$$

$$\log_a b = \frac{1}{\log_b a}$$

$$\log_b 1 = 0$$

$$\log_b b = 1$$

Somatórios

$$a_1 + a_2 + \ldots + a_n = \frac{(a_1 + a_n)n}{2}$$

$$1 + 2 + 3 + \ldots + n = \frac{(1 + n)n}{2}$$

Se $q \neq 1$, então

$$a + aq + aq^2 + \ldots + aq^{n-1} = \frac{a(q^n - 1)}{q - 1}$$

Se $q < 1$, então

$$a + aq + aq^2 + \ldots = \frac{a}{1-q}$$

$$1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$$

$$\sum_{i=1}^{n} \lfloor \log_2 i \rfloor = (n+1)\lfloor \log_2 n \rfloor - 2^{\lfloor \log_2 n \rfloor + 1} = \Theta(n \log n)$$

$$\sum_{i=1}^{n} f(i) \leqslant \int_{x=1}^{x=n+1} f(x)dx$$

Outras fórmulas

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1 + O(1/n))$$

$$\log_2(n!) = \Theta(n \log n)$$

$$\lceil x \rceil = \min\{n : n \in \mathbb{Z} \text{ e } n \geqslant x\}$$

$$\lfloor x \rfloor = \text{máx } \{n : n \in \mathbb{Z} \text{ e } n \leqslant x\}$$

$\lfloor \log_2 k \rfloor + 1$ bits são necessários para representar um inteiro k na base binária.

Apêndice B

Alfabeto Grego

O alfabeto grego abaixo foi tomado da uma página
`http://www.kfish.org/tech/latex/greek-alphabet.html`.

minúscula	comando Latex	maiúscula
α	*alpha*	A
β	*beta*	B
γ	*gamma*	Γ
δ	*delta*	Δ
ϵ, ε	*epsilon*	E
ζ	*zeta*	Z
η	*eta*	H
θ, ϑ	*theta*	Θ
ι	*iota*	I
κ	*kappa*	K
λ	*lambda*	Λ
μ	*mu*	M
ν	*nu*	N
ξ	*xi*	Ξ
o	[omicron]	O
π, ϖ	*pi*	Π
ρ, ϱ	*rho*	P
σ, ς	*sigma*	Σ
τ	*tau*	T
υ	*upsilon*	Υ
ϕ, φ	*phi*	Φ
χ	*chi*	X
ψ	*psi*	Ψ
ω	*omega*	Ω

Apêndice C

Introdução à Teoria dos Grafos

Definição C.1. Um grafo $G = (V, E)$ é um conjunto finito V de vértices (*vertex* em Inglês) e um conjunto finito E de arestas (edges em Inglês) onde cada aresta é um par ordenado de vértices (Ex.: (v, w)).

Isto é, E é uma relação sobre V, $E \subset E^2$.

Um *laço* é uma aresta com ambos os extremos em um mesmo vértice. Duas ou mais arestas são *múltiplas* quando têm o mesmo par de vértices como extremos. Dizemos que um grafo é *simples* quando não possui laços nem arestas múltiplas. Os grafos utilizados neste texto serão todos *simples* a menos de menção em contrário. De fato, a definição de grafo utilizada considera arestas como pares ordenados. Então não poderiamos ter arestas múltimas, já que o conjunto E de arestas não pode ter elementos repetidos (é conjunto!).

Definição C.2. Um grafo $G = (V, E)$ pode ser orientado (dirigido) ou não orientado (não dirigido). Em um grafo orientado, a ordem entre os vértices de uma aresta (v, w) é importante; isto é, podemos ter $(v, w) \in E$ mas $(w, v) \notin E$. Um grafo não orientado é tal que, se $(v, w) \in E$, então $(w, v) \in E$. Isto é, E é uma relação simétrica.

Um grafo orientado ou dirigido é representado graficamente usando bolinhas ou círculos para vértices e setas para arestas, como mostrado na Figura C.1. Nesta figura não são dados nomes aos vértices.

Um grafo não orientado ou não dirigido é representado graficamente usando segmentos de retas para arestas, como mostrado na Figura C.2.

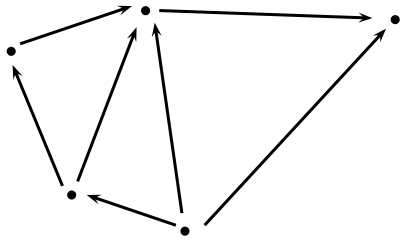


Figura C.1: Representação gráfica de um grafo orientado

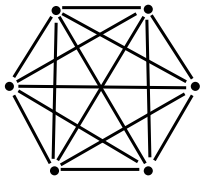


Figura C.2: Representação gráfica de um grafo não orientado

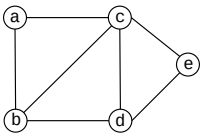
Denotamos por $|V|$ e $|E|$ a cardinalidade dos conjuntos de vértices e arestas de um grafo $G = (V, E)$, respectivamente. No exemplo da Figura C.1, temos $|V| = 5$ e $|E| = 7$. Em grafos não orientados, contamos as duas arestas entre dois vértices apenas uma vez. Assim, no exemplo da Figura C.2, temos $|E| = 15$ e não $|E| = 30$, obtido de $6 * 5$. O *tamanho* de um grafo G é dado por $|V| + |E|$.

Definição C.3. Dada uma aresta $e = (a, b)$, dizemos que os vértices a e b são os *extremos* da aresta e e que a e b são vértices *adjacentes*.

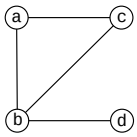
Definição C.4. Dizemos também que a aresta e é *incidente* aos vértices a e b, e que os vértices a e b são *incidentes* à aresta e.

Definição C.5. Um *subgrafo* $H = (V', E')$ de um grafo $G = (V, E)$ é um grafo tal que $V' \subseteq V$ e $E' \subseteq E$. Um *subgrafo gerador* de G é um subgrafo H com $V' = V$.

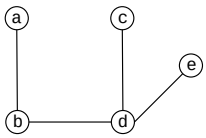
Exemplos:



Grafo G



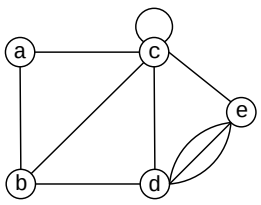
Subgrafo não gerador



Subgrafo gerador

Definição C.6. O *grau* de um vértice v, denotado por $d(v)$ é o número de arestas incidentes a v.

Por esta definição, os laços são contados duas vezes.
Exemplo:



d(a)=2

d(b)=3

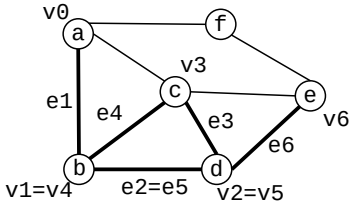
d(c)=6

d(d)=5

d(e)=4

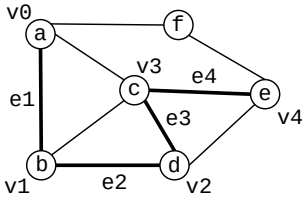
Definição C.7. Um *caminho* P de v_0 a v_n no grafo G é uma seqüência finita e não vazia $(v_0, e_1, v_1, \ldots, e_n, v_n)$ cujos elementos são alternadamente vértices e arestas e tal que, para todo $1 \leq i \leq n$, v_{i-1} e v_i são os extremos de e_i. O *comprimento* do caminho P é dado pelo seu número de arestas, ou seja, n.

Exemplo:

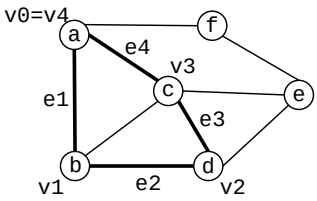


Definição C.8. Um *caminho simples* é um caminho em que não há repetição de vértices e nem de arestas na sequência. Um *ciclo* ou *caminho fechado* é um caminho em que $v_0 = v_n$.

Exemplo:



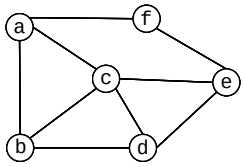
Caminho Simples



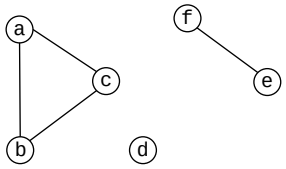
Ciclo

Definição C.9. Dizemos que um grafo é *conexo* ou *conectado* se, para qualquer par de vértices u e v de G, existe um caminho de u a v em G. Caso contrário, o grafo é *não conexo* ou *desconectado*.

Dois vértices u e v de G estão na mesma *componente conexa* de G se há caminho de u a v em G. Um grafo conexo tem uma única componente conexa, já um grafo não conexo tem pelo menos duas componentes conexas.
Exemplo:



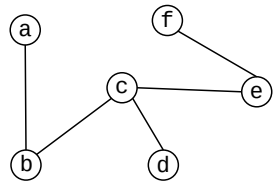
Conexo



Não-conexo com
3 componentes conexos

Definição C.10. Uma **árvore** é um grafo conexo sem ciclos. Uma *folha* de uma árvore é um vértice de grau um.

Exemplo:



Definição C.11. Uma **árvore binária** (AB) é uma árvore dirigida (árvore e grafo dirigido) definido indutivamente como:

- uma AB com um único vértice v é uma árvore. A raiz desta árvore é v;
- se C e D são duas árvores binárias com raízes w e t, e v um vértice não pertencente a C ou D, então o grafo composto por C, D, v e as arestas (v, w) e (v, t) é uma árvore binária. O vértice v é a raiz desta árvore;
- se C é uma AB com raiz w e v um vértice não pertencente a C, então a árvore composta por C, v e a aresta (v, w) é uma AB.

Dizemos que v é o pai de w e t e estes são os filhos de v. Então cada vértice pode ter zero, um ou dois filhos. As árvores C e D são as sub-árvores da árvore binária completa (v com C e D).

Definição C.12. A **altura** de uma árvore binária é definida indutivamente como se segue:

- a altura de uma árvore binária com um vértice é 1;
- a altura de uma AB com raiz v ligada a árvores C e D é 1 + a maior altura entre C e D.

Definição C.13. Uma **árvore binária cheia** (ABCh) é uma árvore binária onde cada vértice tem zero ou dois filhos.

A Figura C.3 mostra um exemplo de uma árvore binária cheia.

Definição C.14. Uma **árvore binária completa** (ABC) é uma árvore binária na qual todas as sub-árvores ligadas a um mesmo vértice possuem a mesma altura.

A Figura C.4 mostra um exemplo de uma árvore binária completa.

Exercícios

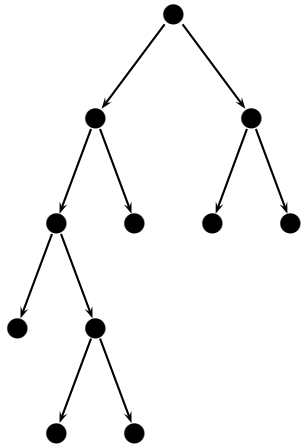


Figura C.3: Exemplo de uma árvore binária cheia

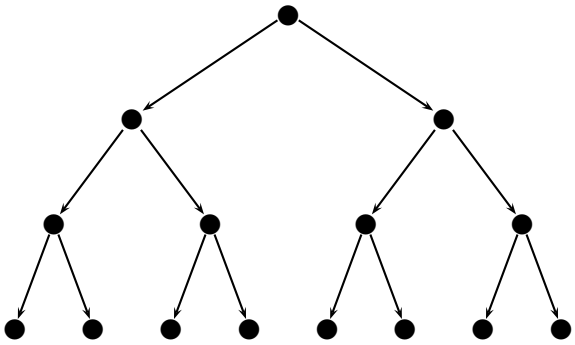


Figura C.4: Exemplo de uma árvore binária completa

C.1. Prove que, para todo grafo $G = (V, E)$ temos:

$$\sum_{v \in V} d(v) = 2|E|.$$

C.2. Explique porquê toda árvore com pelo menos dois vértices tem pelo menos uma folha.

C.3. Prove que um grafo G é uma árvore se e somente se G é conexo com $|V| - 1$ arestas.

C.4. Prove que um grafo G é uma árvore se e somente se G é conexo e a remoção de qualquer aresta desconecta o grafo.

C.5. Prove que um grafo G é uma árvore se e somente se para todo par de vértices u, v de G, existe exatamente um caminho de u a v em G.

Referências Bibliográficas

[1] Bogart, Ken; Drysdale, Scot; Stein, Cliff. Discrete Math for Computer Science Students.

[2] Coniglio, Marcelo E. Teoria Axiomática de Conjuntos: uma Introdução.

[3] Hrbacek, Karel; Jech, Thomas. Introduction to Set Theory. Third Edition, Marcel Dekker, Inc, 1999.

[4] Garnier, Rowan; Taylor, John. Discrete Mathematics for New Technology.

[5] Sampaio, João. Teoria dos Números.

[6] Guimarães, José de Oliveira. Introdução à Lógica Matemática. Disponível em `http://www2.dc.ufscar.br/~jose/courses`

Índice Remissivo