

Capítulo 2

Noções Preliminares

Neste capítulo serão introduzidas algumas noções matemáticas básicas para o entendimento dos demais capítulos. A apresentação do material é feita de modo informal, e o leitor deve procurar na literatura citada nas referências esclarecimentos maiores, quando isto se tornar necessário.

2.1 Conjuntos

As idéias da Matemática, em geral, envolvem um processo evolucionista no qual vários estudiosos trabalham paralelamente. Entretanto, a Teoria dos Conjuntos [26, 27] não compartilha esta característica com as demais áreas da Matemática, pois ela foi criada pelo matemático russo-alemão chamado George Cantor¹. Em 1872, Cantor conheceu o matemático Richard Dedekind, cujo pensamento abstrato e lógico influenciou as idéias desenvolvidas por Cantor, e que mais tarde iriam al-

¹George Ferdinand Ludwig Philipp Cantor nasceu em 03 de março de 1845 e morreu em 06 de janeiro de 1918. Nascido na Rússia, mudou-se para Alemanha com dez anos de idade. Foi responsável por fazer a distinção entre conjuntos enumeráveis e não enumeráveis. Provou que o conjunto dos números racionais \mathbb{Q} é enumerável e que o conjunto dos números reais \mathbb{R} é não enumerável, usando o célebre argumento da diagonal de Cantor. Foi o primeiro a utilizar o símbolo \mathbb{R} como representação dos conjuntos reais. Durante boa parte de sua vida sofreu ataques de depressão que o conduziram a morte em um hospital psiquiátrico. A descoberta do Paradoxo de Russell contribuiu de forma significativa para a sua falência nervosa.

terar o que hoje se conhece com Matemática Moderna. Em um artigo de 1874 no Crelle's Journal, ele demonstrou que os números reais têm uma correspondência um para um com os números naturais, enquanto que para estes últimos não existe tal correspondência. Sob esta ótica, o ato de contar é um aspecto comum entre a Teoria dos Conjuntos e a Computação, e por este motivo, torna-se desejável rever alguns conceitos iniciais sobre a mesma.

Um conjunto é uma coleção de objetos distintos, usualmente caracterizado por enumeração ou por uma propriedade que seus elementos *possuem, gozam, ou satisfazem*. Conjuntos são denotados por letras maiúsculas latinas ou gregas, com ou sem índices, assim A , Γ e B_1 podem ser usados como nomes de conjuntos. Os objetos que constituem um conjunto A são membros ou elementos do conjunto.

Com respeito à notação, deve-se estabelecer que:

1. se a é um elemento de A , diz-se que a pertence a A ou $a \in A$; abreviadamente, se vários elementos, digamos, a, b e c são elementos de um conjunto A , pode-se dizer $a, b, c \in A$;
2. se um conjunto A tem como únicos elementos a, b e c , podemos representá-lo por $A = \{a, b, c\}$;
3. uma propriedade que certos elementos gozam é representada por $P(x)$. Se forem considerados valores para x , por exemplo 1, representado por $P(1)$, le-se “ P de 1”. Assim o conjunto cujos elementos satisfazem uma propriedade P é representado por $A = \{x \in B | P(x)\}$. Conjuntos especificados desta forma são lidos como: “ A é o conjunto dos elementos x de B tal que $P(x)$ ”;
4. se os elementos de um conjunto são indexados, por exemplo pelos números naturais de 1 a n , usamos a notação $A = \{a_1, a_2, \dots, a_n\}$; se o conjunto de índices de A for um outro conjunto, digamos I , cujos elementos não foram especificados, dizemos $A = \{a_i\}_{i \in I}$.

Existem conjuntos que possuem um grande número de elementos, por exemplo o conjunto de todos os jornais de todas as cidades do mundo que foram publica-

dos desde o início da imprensa até o dia de hoje. Note que embora não saibamos o número de elementos, estes estão bem especificados por uma propriedade definidora.

Exemplo 2.1

pares $\{x \in \mathbb{N} \mid x \text{ é um número natural e } x \text{ é divisível } 2\}$

ímpares $\{x \in \mathbb{N} \mid x \text{ é um número natural e } x \text{ não é divisível } 2\}$

Um conjunto que não tem elementos é dito ser vazio, e é denotado por \emptyset . Conjuntos vazios em geral surgem quando é especificado por uma propriedade que não é satisfeita por nenhum elemento. Por exemplo $A = \{x \mid x \neq x\}$.

Definição 2.1

1. Diz-se que A é um subconjunto de B se e somente se para todo x , se $x \in A$ então $x \in B$ e denotamos por $A \subseteq B$; neste caso diz-se também que B é um superconjunto de A , denotado por $B \supseteq A$. Formalmente tem-se² $A \subseteq B \Leftrightarrow \text{para todo } x, \text{ se } x \in A \text{ então } x \in B$.
2. Diz-se que A é igual a B , o que é denotado por $A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$. Formalmente $A = B \Leftrightarrow A \subseteq B \text{ e } B \subseteq A$.
3. Diz-se que A é um subconjunto próprio de B , o que é denotado por $A \subset B$, se e somente se A é um subconjunto de B , mas A não é igual a B . Formalmente $A \subset B \Leftrightarrow A \subseteq B \text{ e } B \not\subseteq A$.

Exemplo 2.2 $\{a, b, c\} \subset \{b, c, a, e\}$; $\text{pares} \subset \mathbb{N}$, $\text{ímpares} \subset \mathbb{N}$.

Lema 2.1 São válidas as seguintes propriedades:

$$(p1) \quad A \subseteq B \text{ e } B \subseteq C \Rightarrow A \subseteq C$$

$$(p2) \quad A \subset B \text{ e } B \subset C \Rightarrow A \subset C$$

$$(p3) \quad A \subset B \text{ e } B \subset A \Rightarrow A = B$$

²Neste capítulo é utilizado \Leftrightarrow para representar a expressão “se e somente se” e \Rightarrow para representar a expressão “se...então...”.

Demonstração (p1): Uma vez que $A \subseteq B$ e $B \subseteq C$ tem-se

$$\left. \begin{array}{l} \forall x \in A \rightarrow x \in B \\ \forall x \in B \rightarrow x \in C \end{array} \right| \Rightarrow \begin{array}{l} \forall x \in A \rightarrow x \in C \\ A \subseteq C \end{array}$$

Demonstração (p2): Uma vez que $A \subset B$ e $B \subset C$ tem-se

$$\left. \begin{array}{l} (i) \forall x \in A \rightarrow x \in B \\ (ii) \exists y \in B \mid y \notin A \\ (iii) \forall y \in B \rightarrow y \in C \\ (iv) \exists z \in C \mid z \notin B \end{array} \right| \Rightarrow \begin{array}{l} (i) \text{ e } (iii) \forall x \in A \rightarrow x \in C \\ (iv) \text{ e } (ii) \exists z \in C \mid z \notin A \\ A \subset C \end{array}$$

Demonstração (p3): $\forall x \in A \rightarrow x \in B$, mas se $z \in B$, não necessariamente $z \in A$.
 $\forall z \in B \rightarrow z \in A$, logo para satisfazer a condição anterior $A = B$.

Definição 2.2 [Conjunto potência] Seja A um conjunto. O conjunto de subconjuntos de A é chamado de conjunto das partes de A ou conjunto potência de A , denotado por $\wp(A)$. Formalmente $\wp(A) = \{X \mid X \subseteq A\}$.

Note que $\wp(A)$ é um conjunto de conjuntos, diz-se que tais conjuntos são famílias de conjuntos.

Definição 2.3 [Operações sobre conjuntos]

União Sejam A e B conjuntos. A união de A e B denotada por $A \cup B$ é definida por $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$. Seja $\{A_i\}_{i \in I}$ uma família de conjuntos com índice I . Então a união da família é definida por

$$\bigcup_{i \in I} A_i = \{x \mid \text{existe } i \in I \text{ tal que } x \in A_i\}$$

Se $I = 1, 2, \dots, n$ escreve-se

$$\bigcup_{i=1}^{i=n} A_i \text{ ou } \bigcup_{i=1}^n A_i$$

Interseção Sejam A e B conjuntos. A interseção de A e B denotada por $A \cap B$ é definida por $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$. Seja $\{A_i\}_{i \in I}$ uma família de conjuntos com índice I . Então a interseção da família é definida por

$$\bigcap_{i \in I} A_i = \{x \mid \text{para todo } i \in I \text{ } x \in A_i\}$$

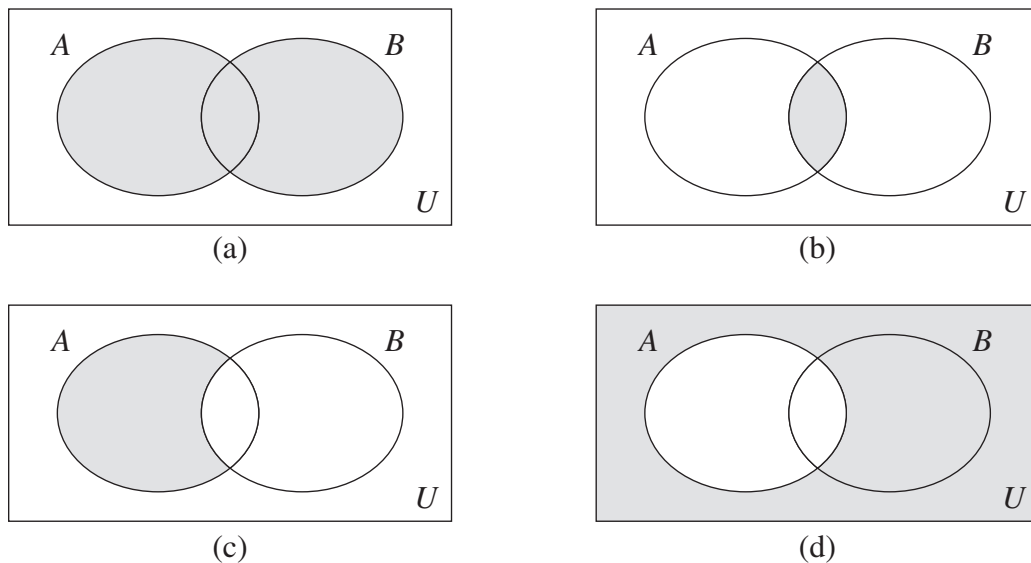


Figura 2.1: Diagrama de Venn de operações com conjuntos: (a) $A \cup B$; (b) $A \cap B$; (c) $A - B$; (d) \bar{A} .

Se $I = 1, 2, \dots, n$ escreve-se

$$\bigcap_{i=1}^{i=n} A_i \text{ ou } \bigcap_{i=1}^n A_i$$

Diferença Sejam A e B conjuntos. A diferença de A e B , denotada por $A - B$, é definida por $A - B = \{x \mid x \in A \text{ e } x \notin B\}$.

Complemento Seja A um conjunto. O complemento de A , denotado por \bar{A} , é definido por $\bar{A} = \{x \mid x \notin A\}$.

Potência Seja A um conjunto. O conjunto potência de A (também conhecido como conjunto das partes de A), denotado por \mathcal{P} , é definido por $\mathcal{P} = \{x \mid x \subseteq A\}$.

Em geral, serão estudadas propriedades de subconjuntos de um conjunto U ou “conjunto universo”. Portanto, nas definições feitas até o momento, presupõe-se sempre que para um conjunto $A \subseteq U$, $A = \{x \in U \mid P(x)\}$. No caso do complemento de A , $\bar{A} = U - A$. Alguns autores se referem à diferença $A - B$ como o complemento de B com relação a A . A figura 2.1 apresenta diagramas de Venn ilustrativos das operações de união, interseção, diferença e complemento.

Exemplo 2.3

1. $\{1, 2, 3\} \cup \{3, 4\} = \{1, 2, 3, 4\}$
2. $\{1, 2, 3, 5\} \cap \{3, 4, 5\} = \{3, 5\}$
3. $\{1, 2, 3\} - \{3, 4\} = \{1, 2\}$
4. $\overline{\text{pares}} = \text{ímpares}$, com relação a \mathbb{N}

Lema 2.2 São válidas as seguintes propriedades:

- (p4) $A \subseteq B \Rightarrow A \cup B = B$
- (p5) $A \subseteq B \Rightarrow A \cap B = A$
- (p6) $A \subseteq B \Rightarrow \bar{B} \subseteq \bar{A}$
- (p7) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (p8) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (p9) $\overline{A \cup B} = \bar{A} \cap \bar{B}$
- (p10) $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Ainda que o formalismo matemático sugira uma Teoria dos Conjuntos completa e consistente, o leitor deve ter cuidado para não aceitá-la de forma incondicional e ingênua. Bertrand Russell descobriu um paradoxo na teoria (Paradoxo de Russell) que nunca foi resolvido. Considere o conjunto C como sendo "o conjunto de *todos* os conjuntos que não se contêm a si próprios como membros". Formalmente, A é elemento de C se e só se A não é elemento de A , isto é, $C = \{A | A \notin A\}$.

Pela Teoria dos Conjuntos, C é um conjunto perfeitamente bem definido. Contudo, se C contém a si mesmo, então, por definição, ele não é membro de C . Por outro lado, supondo que C não contenha a si mesmo, então ele precisa ser elemento de C , uma declaração aparentemente verdadeira que leva a uma contradição lógica.

Outra formulação interessante deste paradoxo é conhecida como paradoxo do barbeiro. Imagine um barbeiro que recebe a atribuição de barbear todos os homens, e somente homens quem não barbeiam a si mesmos. Observe que existem apenas dois conjuntos distintos, aquele no qual os homens barbeiam a si mesmos, e aquele no qual os homens não barbeiam a si mesmos. Se o barbeiro pertence ao conjunto dos homens que barbeiam a si mesmo, então ele, como barbeiro não poderia se barbear. Ora, mas como ele não pode se barbear, então ele, como barbeiro, deve cumprir sua obrigação de se barbear. Parece evidente que a única solução para este

problema, é que o problema não deveria existir.

Kurt Gödel usou o paradoxo do barbeiro para provar o seu teorema da incompletude. Alan Turing também demonstrou a indecidibilidade do problema da parada usando o mesmo paradoxo.

2.2 Funções

A Computação emprega funções em larga escala, particularmente aquelas que transformam um conjunto finito em outro conjunto finito, funções estas conhecidas como funções discretas. Um programa de computador pode ser entendido como uma função que utiliza dados como argumentos de entrada, e que produz um resultado associado a estes argumentos.

Sejam A e B conjuntos quaisquer; uma função f de A em B é uma *regra* que associa a certos elementos de A um único elemento de B . Esta unicidade significa que se f associa $a \in A$ a $b_1 \in B$ e a $b_2 \in B$ então $b_1 = b_2$.

Para dizer que f é uma função de A em B usa-se a notação $f : A \rightarrow B$. O conjunto de todas as funções de A em B é denotado por B^A , ou seja $B^A = \{f \mid f : A \rightarrow B\}$.

Seja A um conjunto, então chama-se de operação n -ária uma função $f : A^n \rightarrow A$.

Se $f : A \rightarrow B$ então diz-se que A é o conjunto de partida de f e B o conjunto de chegada de f . O subconjunto de A cujos elementos são associados a elementos de B é chamado de domínio de f , denotado por $dom(f)$. O conjunto B , por sua vez é chamado de contra-domínio de f , denotado por $ctr(f)$. O subconjunto de B , aos quais aqueles elementos de A foram associados, é chamado de imagem de f , que denota-se por $img(f)$. Denota-se o elemento de B associado a um elemento $a \in A$ por $f(a)$, tal como a Figura 2.2.

Definição 2.4 Seja $f : A \rightarrow B$ e $g : A \rightarrow B$. Diz-se que

1. f é uma sobrejeção, ou que f é uma função de A sobre B , se e somente se

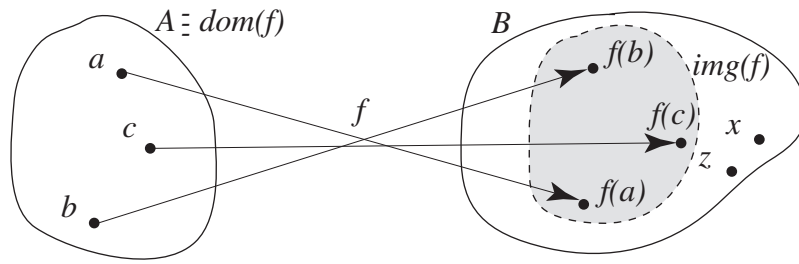


Figura 2.2: Função de A em B .

$img(f) = B$ (ver Figura 2.3a).

2. f é uma injeção ou injetiva de A em B se e somente se para cada elemento do conjunto A corresponde um elemento distinto do conjunto B , isto é, para todo $x, y \in A$ se $f(x) = f(y)$ então $x = y$ (ver Figura 2.3b).
3. f é uma bijeção se e somente se f é uma injeção e uma sobrejeção.
4. f é igual a g , denotado por $f = g$ se e somente se para todo $x \in dom(f)$ $f(x) = g(x)$, e além disso $dom(f) = dom(g)$
5. f é uma função total de A em B se e somente se $dom(f) = A$.
6. f é uma função parcial de A em B se nem todos os $x \in A$ pertencem ao $dom(f)$.
7. se $x \in dom(f)$ então $f(x) \downarrow$ (f converge em x); se $x \in A - dom(f)$ então $f(x) \uparrow$ (f diverge em x).

Exemplo 2.4 A seguir são exibidos alguns tipos de funções:

Funções no discreto Por exemplo funções do conjunto dos naturais \mathbb{N} no conjunto dos naturais $f : \mathbb{N} \rightarrow \mathbb{N}$

1. $f : \mathbb{N} \rightarrow \mathbb{N}$, definida por: para todo $x \in \mathbb{N}$ $f(x) = x + 1$
2. $f : \mathbb{N} \rightarrow \mathbb{N}$, definida por: para todo $x \in \mathbb{N}$ $f(x) = 2.x$
3. $f : \mathbb{N} \rightarrow \mathbb{N}$, definida por: para todo $x \in \mathbb{N}$, tal que 3 divide x $f(x) = x/3$

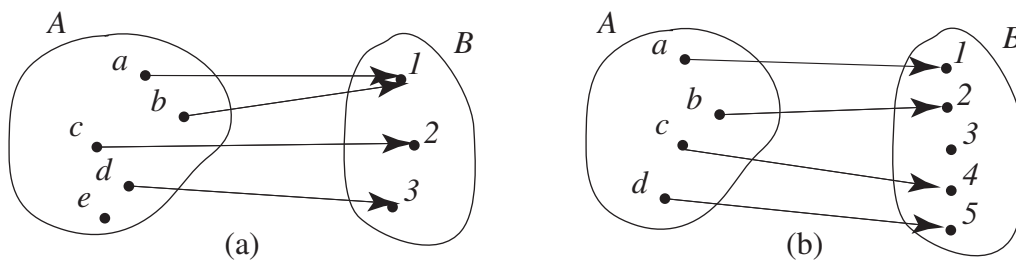


Figura 2.3: Funções: (a) Sobrejetora; (b) Injetora.

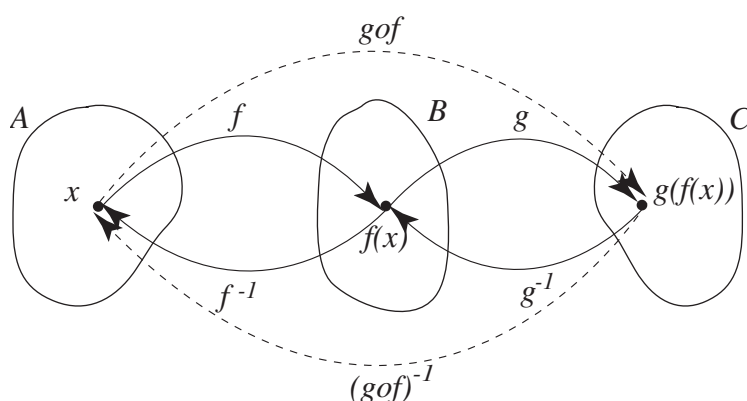


Figura 2.4: Composição de f e g .

As funções 1. e 2. são funções totais não sobrejetivas, 3. é uma função parcial pois $\text{dom}(f) = \{0, 3, 6, 9, \dots\}$

Funções no contínuo Por exemplo funções $f : \mathbb{R} \rightarrow \mathbb{R}$, onde \mathbb{R} é o conjunto dos reais.

Definição 2.5 Seja $f : A \rightarrow B$ uma função injetiva. A inversa de f , denotada por f^{-1} é uma função de B em A definida por $f^{-1}(x) = y$ se e somente se $f(y) = x$. Formalmente $f^{-1}(x) = y \Leftrightarrow f(y) = x$.

Definição 2.6 Sejam as funções $f : A \rightarrow B$ e $g : B \rightarrow C$. A composição de f e g , $g \circ f$, é a função de A em C tal que $g \circ f(x) = g(f(x))$ (ver Figura 2.4).

Lema 2.3 Sejam as funções $f : A \rightarrow B$ e $g : B \rightarrow C$ funções injetivas. Então $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (ver Figura 2.4).

Definição 2.7 Seja $A \subseteq B$ um conjunto. Uma função $f : A \rightarrow \{0, 1\}$ é a função característica para A se e somente se

$$\text{para todo } x \in B \quad f(x) = \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

Funções características de um conjunto A são, em geral, representadas por χ_A .

Exemplo 2.5 Se o resto da divisão de x por y for dado por $\text{resto}(x, y)$ então a seguinte função é a função característica do conjunto dos números ímpares:

$$\chi_{\text{ímpares}}(x) = \text{resto}(x, 2)$$

e para os pares:

$$\chi_{\text{pares}}(x) = 1 - \text{resto}(x, 2)$$

Se este processo pode ser representado por uma função sobrejetora $h : \mathbb{N} \rightarrow A$, onde h associa a cada número natural um elemento de A , então diz-se que A é contável, caso contrário é não contável. Se o processo de contagem termina, ou seja, se existe uma bijeção $h : \{1, \dots, n\} \rightarrow A$, $n \in \mathbb{N}$, diz-se que a cardinalidade de A , denotado por $\#(A)$, é n (finita). O Algoritmo 2.1 apresenta um resolutor para o processo de contagem.

Data: Conjunto A cuja quantidade de elementos deseja-se obter

Result: Cardinalidade finita do conjunto A

iContagem = 0;

while $A \neq \emptyset$ **do**

Retirar um elemento de A ;

iContagem = iContagem + 1;

end

Cardinalidade finita do conjunto = iContagem;

Algoritmo 2.1: Determinação da cardinalidade finita de um conjunto

Se o processo de contagem não termina, diz-se que A tem cardinalidade infinita. Por exemplo todo subconjunto de \mathbb{N} tem cardinalidade infinita que é representada por \aleph_0 (aleph 0). Na realidade, no caso de \mathbb{N} , após a retirada de n elementos não importante quão grande é n ainda sobrá um conjunto com cardinalidade \aleph_0 . O conjunto dos pares e o dos ímpares também têm cardinalidade \aleph_0 , e ambos são

partes de \mathbb{N} . Observe que se um conjunto pode ser colocado em correspondência biunívoca, então ele também possui cardinalidade \aleph_0 .

Definição 2.8 Um conjunto A é enumerável (contável) se ele é finito ou se tem cardinalidade \aleph_0 . Uma enumeração para um conjunto χ enumerável infinito representado por uma seqüência $\chi = a_1, a_2, a_3, \dots$ é uma bijeção $f(a_i) = i \in \mathbb{N}$.

Exemplo 2.6 \mathbb{Z} é enumerável.

$$f : \mathbb{Z} \rightarrow \mathbb{N}$$

$$f(n) = \begin{cases} 2n + 1 & , \text{ se } n \geq 0 \\ -2n & , \text{ se } n < 0 \end{cases}$$

□

Exemplo 2.7 Pares ordenados envolvendo números naturais, $\mathbb{N} \times \mathbb{N}$ é enumerável. Para demonstrar, basta ordenar os pares ordenados como se segue e em seguida atribuir etiquetas de números naturais às suas posições.

$$\begin{array}{ccccccc} \swarrow & & & & & & \\ \langle 1, 1 \rangle & \langle 1, 2 \rangle & \langle 1, 3 \rangle & \langle 1, 4 \rangle & \dots & & \\ \swarrow & & & & & & \\ \langle 2, 1 \rangle & \langle 2, 2 \rangle & \langle 2, 3 \rangle & \langle 2, 4 \rangle & \dots & & \\ \swarrow & & & & & & \\ \langle 3, 1 \rangle & \langle 3, 2 \rangle & \langle 3, 3 \rangle & \langle 3, 4 \rangle & \dots & & \\ \swarrow & & & & & & \\ \langle 4, 1 \rangle & \langle 4, 2 \rangle & \langle 4, 3 \rangle & \langle 4, 4 \rangle & \dots & & \\ & \vdots & \vdots & \vdots & \vdots & & \end{array}$$

□

Exemplo 2.8 O conjunto de todas as palavras formadas a partir de um alfabeto $\Sigma = \sigma_1, \sigma_2, \dots, \sigma_n$, conhecido por Σ^* , é enumerável pela função:

$$f : \Sigma^* \rightarrow \mathbb{N}$$

$$f(\text{palavra}) = \sum_{i=1}^k \text{posição do caracter}_i \times n^i$$

onde k é o tamanho da palavra.

□

Exemplo 2.9 O conjunto dos programas de qualquer linguagem de programação (LP) é enumerável, pois qualquer LP possui um alfabeto Σ tal que o programa está em Σ^* .

□

Definição 2.9 Um conjunto A é dito não enumerável se $\#(A) > \aleph_0$.

A prova da existência de conjuntos não enumeráveis foi feita por Cantor (1874) através de um método que ficou conhecido como diagonalização de Cantor, ilustrado no exemplo a seguir.

Exemplo 2.10 O conjunto \mathbb{R} é não enumerável. A idéia para essa demonstração é que se existir uma bijeção $\mathbb{R} \rightarrow \mathbb{N}$, seria possível compor uma bijeção de $]0, 1[\rightarrow \mathbb{R}$ e então concluir que $]0, 1[$ é enumerável. Contudo, sabe-se que $]0, 1[$ não é enumerável. Assim, suponha uma demonstração por contradição. Suponha que $]0, 1[$ é enumerável, e seja uma bijeção $f : \mathbb{N} \rightarrow]0, 1[$. Assim, cada número natural n é mapeado sobre um número decimal:

$$\begin{array}{lcl} 0 & \mapsto & 0. a_{00} a_{01} a_{02} \\ 1 & \mapsto & 0. a_{10} a_{11} a_{12} \\ 2 & \mapsto & 0. a_{20} a_{21} a_{22} \\ \vdots & & \vdots \end{array}$$

A intenção é mostrar que f não é uma bijeção. A idéia de que \mathbb{N} tem cardinalidade \aleph_0 , é preciso mostrar que $]0, 1[$ tem cardinalidade maior que \aleph_0 . Desta forma, o argumento será que f não pode ser sobrejetora, logo é possível encontrar um número que não é mapeado.

$$\begin{array}{lcl} 0 & \mapsto & 0. \mathbf{a}_{00} a_{01} a_{02} \\ 1 & \mapsto & 0. a_{10} \mathbf{a}_{11} a_{12} \\ 2 & \mapsto & 0. a_{20} a_{21} \mathbf{a}_{22} \\ \vdots & & \vdots \end{array}$$

onde $b = 0.b_0b_1b_2 \dots$ e $b_0 \neq a_{00}, b_1 \neq a_{11}, \dots, b_i \neq a_{ii}$

Suponha $i \in \mathbb{N}$ tal que $f(i) = b$. Note que $f(i)$ é mapeado sobre o número real $0.a_{i0}a_{i1}a_{i2} \dots a_{ii} \dots$. Porém, por construção de b , $b_i \neq a_{ii}$, logo $f(i) \neq b$. Assim, tem-se que b não está mais na lista. Se b não está na lista, f não é sobrejetora, e também não é bijetora. \square

Teorema 2.1 Seja A um conjunto qualquer, $\#(A) = \aleph_i$. Então $\#(\mathcal{P}(A)) > \#(A)$ e $\#(\mathcal{P}(A)) = \aleph_{i+1}$.

Basta provar que $\#(A) \leq \#(\mathcal{P}(A))$. Para isso, é suficiente mostrar que não existe função bijetora de $A \rightarrow \mathcal{P}(A)$. Seja então uma $f : A \rightarrow \mathcal{P}(A)$ bijetiva. Seja $x \in A$ de modo que $f(x) = y'$, onde $\#(y') = 1$. Observe que todos os elementos de A estão mapeados sobre os elementos de $\mathcal{P}(A)$ com cardinalidade 1. Resta mapear os elementos de $\mathcal{P}(A)$ cuja cardinalidade é maior que 1. Como todos os elementos de A já foram utilizados, é necessário tomar novamente um x de modo que $f(x) = y''$ onde $\#(y'') > 1$. Contudo, para fazer isto, tem-se um $x \in A$ tal que $f(x) = y'$ e $f(x) = y''$, logo f não é uma função e muito menos bijetiva. \square

Neste sentido, conjuntos infinitos de cardinalidades sucessivamente maiores podem ser obtidos pela aplicação sucessiva da operação conjunto-potência. Considere os conjuntos $A, B = \mathcal{P}(A), C = \mathcal{P}(B), D = \mathcal{P}(C)$ etc. Então, $\#(A) < \#(B) < \#(C) < \#(D) < \dots$. De acordo com a teoria de Cantor, \aleph é o conjunto que possui a menor cardinalidade entre todos os conjuntos infinitos, a qual é denotada por \aleph_0 , o primeiro número da sua série transfinita. Por consequência, $\aleph < \mathcal{P}(\aleph)$.

Teorema 2.2 Sejam A e B dois conjuntos, $B \subseteq A$. Se $\#(A) = \aleph_0$, então $\#(A) \leq \aleph_0$.

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

$$\begin{array}{ccccccc}
 B : & - & a_1 & - & \dots & a_n & \dots \\
 f_2 : & & \downarrow & & & \downarrow & \\
 A : & a_0 & a_1 & a_2 & \dots & a_n & \dots \\
 f_1 : & \downarrow & \downarrow & \downarrow & & \downarrow & \\
 \mathbb{N} : & 1 & 2 & 3 & \dots & n & \dots
 \end{array}$$

Observe também que se B é subconjunto de A , é possível associar cada elemento de B ao mesmo elemento de A através de uma função injetora e total f_2 . Já a composição das funções f_1 e f_2 mostra que existe uma função injetora e total de B para \mathbb{N} . Logo, $\#(B) \leq \#(\mathbb{N})$, ou seja, $\#(B) \leq \aleph_0$. Em outras palavras, qualquer subconjunto (finito ou infinito) de um conjunto enumerável é também um conjunto enumerável. \square

Teorema 2.3 Sejam A e B dois conjuntos quaisquer. Se $\#(A) = \aleph_0$ e $\#(B) = \aleph_0$, então $\#(A \cup B) = \aleph_0$.

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

$$\begin{aligned} A : & a_0, a_1, a_2, \dots, a_{n-1}, a_n, a_{n+1}, \dots \\ B : & b_0, b_1, b_2, \dots, b_{n-1}, b_n, b_{n+1}, \dots \end{aligned}$$

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

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

Desta forma, $A \cup B$ é um conjunto enumerável e $\#(A \cup B) = \aleph_0$, e a união de dois conjuntos enumeráveis é sempre um conjunto enumerável. \square

Teorema 2.4 Sejam A e B dois conjuntos quaisquer. Se $\#(A) = \aleph_0$ e $\#(B) = \aleph_0$, então $\#(A \cap B) \leq \aleph_0$.

Se $A \subseteq B$, então $A \cap B = A$ e $\#(A \cap B) = \#(A) = \aleph_0$ por hipótese. Se, por outro lado, $B \subseteq A$, então $A \cap B = B$ e $\#(A \cap B) = \#(B) = \aleph_0$ por hipótese. Finalmente, se nenhuma dessas duas condições for verdadeira, então $(A \cap B) \subseteq A$ e, pelo Teorema 2.2, $\#(A \cap B) \leq \aleph_0$. Portanto, em qualquer caso $\#(A \cap B) \leq \aleph_0$. \square

Teorema 2.5 Sejam A e B dois conjuntos, $B \subseteq A$. Se $\#(A) = \aleph_1$ e $\#(B) = \aleph_0$, então $\#(A - B) = \aleph_1$.

Suponha-se que $\#(A - B) = \aleph_0$. Então, de acordo com o Teorema 2.3, $\#((A - B) \cup B) = \aleph_0$, o que contradiz a hipótese de que $\#(A) = \aleph_1$, pois $(A - B) \cup B = A$. Como $B \subseteq A$, e portanto, $\#(B) \leq \#(A)$, conclui-se que $\#(A - B) = \aleph_1$. \square

2.3 Relações

Freqüentemente, é utilizado a noção de relações entre duas ou mais coisas. Por exemplo, Batman se relaciona com Robin como parceiro; UFRJ e Rio de Janeiro como localização ou, a relação de “estar entre” pode ser verificada entre três objetos quaisquer do espaço físico. Informalmente é exigido que exista uma conexão entre

as coisas que se relacionam. Esta idéia vaga de conexão é incorporada formalmente pelo conceito de *par ordenado*. Fundamentalmente, um par ordenado $\langle a, b \rangle$ possui a seguinte propriedade³:

$$\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle \text{ se e somente se } x_1 = y_1 \text{ e } x_2 = y_2$$

A noção de par ordenado é estendida pela noção de n -tupla ordenada, denotada por $\langle a_1, a_2, \dots, a_n \rangle$ com a propriedade:

$$\langle x_1, x_2, \dots, x_n \rangle = \langle y_1, y_2, \dots, y_n \rangle \Leftrightarrow x_1 = y_1, \dots, x_n = y_n$$

Em vez de n -tupla ordenada diz-se também n -*pla* ou em geral *pla*. Por razões de economia e facilidade de escrita e leitura, representa-se as *plas* de letras indexadas $\langle x_1, x_2, \dots, x_n \rangle$ por \underline{x}_n , considerando o primeiro elemento como possuindo índice 1 e o último índice n .

Definição 2.10 [Produto Cartesiano] Sejam A e B conjuntos. Define-se o produto cartesiano⁴ de A e B , denotado por $A \times B$ como sendo o conjunto de todos os pares ordenados $\langle x, y \rangle$ com $x \in A$ e $y \in B$, ou seja, $A \times B = \{ \langle x, y \rangle \mid x \in A \text{ e } y \in B \}$.

Exemplo 2.11 Seja $A = \{0, 1\}$ e $B = \{1, 2, 3\}$ dois conjuntos quaisquer. O produto cartesiano de A por B , e vice-versa, é dado por:

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

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

Se A e B são conjuntos então uma relação binária R entre A e B é qualquer subconjunto do produto cartesiano de A e B , ou seja $R \subseteq A \times B$. Quando $A = B$ diz-se que R é uma relação em A ou $R \subseteq A^2$. A Figura 2.5 mostra: (i) os planos coordenados e uma região representando uma relação; (ii) o grafo da relação binária $R = \{ \langle a, b \rangle, \langle a, c \rangle, \langle b, d \rangle, \langle a, d \rangle, \langle c, d \rangle, \langle d, e \rangle \}$.

³Esta propriedade é derivada da definição formal de par ordenado $\langle a, b \rangle = \{ \{a\}, \{a, b\} \}$, veja [28]

⁴O nome cartesiano é uma homenagem a René Descartes, quem historicamente representou funções utilizando eixos ortogonais, o eixo horizontal representando o domínio da função e o vertical o contradomínio. Assim qualquer região destes planos de coordenadas é uma relação, incluindo as funções.

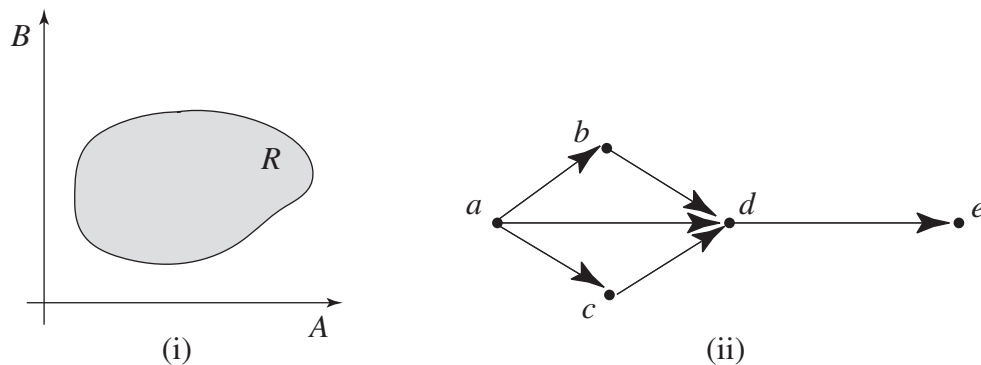


Figura 2.5: Relações: (i) os planos coordenados e uma região representando uma relação; (ii) o grafo da relação binária $R = \{ \langle a, b \rangle, \langle a, c \rangle, \langle b, d \rangle, \langle a, d \rangle, \langle c, d \rangle, \langle d, e \rangle \}$.

Do mesmo modo pode-se definir relações n -árias em uma família de conjuntos $\{A_i\}_{1 \leq i \leq n}$, como qualquer subconjunto R do produto cartesiano, isto é,

$$\prod_{i=1}^n A_i$$

O natural n é a *aridade* da relação R .

Definição 2.11 [Composição] Sejam A , B e C conjuntos, R uma relação em $A \times B$ e S uma relação em $B \times C$. Então, a composição $S \circ R$ é uma relação em $A \times C$ definida por $\{ \langle a, c \rangle \mid \langle a, b \rangle \in R \text{ e } \langle b, c \rangle \in S \}$, e ilustrada na Figura 2.6.

A forma tradicional de representação de uma relação é através das n -tuplas ordenadas. Entretanto, existem outros modos de representação que privilegiam determinados tipos de visão, particularmente no que diz respeito às propriedades das relações que serão descritas na seção a seguir.

A representação gráfica, por exemplo, privilegia a noção de espacialização da relação. Supondo a e b elementos de um conjunto A , e R uma relação de A em A tem-se que existirá uma seta entre a e b , se e somente se, $\langle a, b \rangle \in R$. A Figura 2.7 apresenta a espacialização de uma relação em A^2 . Neste caso a relação é dada por $R = \{ \langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 3, 3 \rangle \}$.

A representação matricial das relações é interessante, sob o ponto de vista matemático, sempre que a complexidade da representação gráfica dificulta a compreensão da relação. Assim, seja $A = \{a_1, a_2, \dots, a_n\}$ e $B = \{b_1, b_2, \dots, b_m\}$ conjuntos

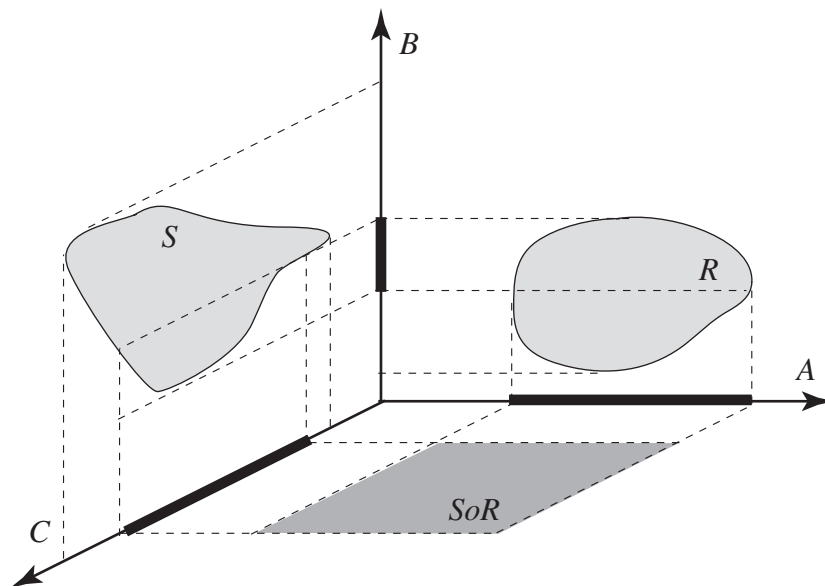


Figura 2.6: Composição de R e S , dada por $S \circ R$.

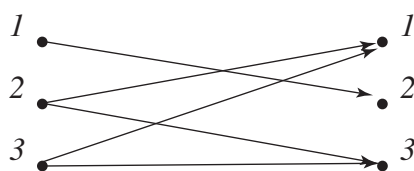


Figura 2.7: Representação gráfica de uma relação.

quaisquer tais que $R: A \rightarrow B$. A matriz $M_{n \times m}$, representativa da relação R é dada por:

$$\begin{array}{ll} M[i, j] = F, & \langle a_i, b_j \rangle \notin R \\ & V, \quad \langle a_i, b_j \rangle \in R \end{array}$$

Exemplo 2.12 A Relação $R = \{\langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 3, 3 \rangle\}$, descrita na Figura 2.7, pode ser escrita na forma matricial:

$$R = \begin{bmatrix} F & V & F \\ V & F & V \\ V & F & V \end{bmatrix}$$

Exemplo 2.13 A Relação $S = \{\langle 1, a \rangle, \langle 1, b \rangle, \langle 2, a \rangle, \langle 3, b \rangle\}$, sobre os conjuntos $A = \{1, 2, 3\}$ e $B = \{a, b\}$ 2.7, pode ser escrita na forma matricial:

$$S = \begin{bmatrix} V & V \\ V & F \\ F & V \end{bmatrix}$$

Definição 2.12 [Matriz Produto Lógico] Seja uma relação R com matriz de representação $M_R(m \times n)$, e uma relação S com matriz de representação $M_S(n \times p)$. A relação $S \circ R$ possui uma matriz de representação $M_{S \circ R}(m \times p)$ tal que:

$$\begin{aligned}
M_{S \circ R}[i, j] &= [M_R(i, 1) \wedge M_S(1, j)] \vee \\
&\quad [M_R(i, 2) \wedge M_S(2, j)] \vee \\
&\quad \dots \vee \\
&\quad [M_R(i, n) \wedge M_S(n, j)]
\end{aligned}$$

onde $i \in \{1, \dots, m\}$ e $j \in \{1, \dots, p\}$.

Exemplo 2.14 Seja a relação $R = \{\langle 1, 2 \rangle, \langle 2, 1 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 3, 3 \rangle\}$, e a relação $S = \{\langle 1, a \rangle, \langle 1, b \rangle, \langle 2, a \rangle, \langle 3, b \rangle\}$. A aplicação da relação R , seguida da aplicação S irá produzir a relação $S \circ R = \{\langle 1, a \rangle, \langle 2, a \rangle, \langle 2, b \rangle, \langle 3, a \rangle, \langle 3, b \rangle\}$ (sugere-se ao leitor

utilizar a representação gráfica para obter $S \circ R$). Utilizando-se a matriz produto lógico, pode-se obter facilmente a relação $S \circ R$ através da mera multiplicação das representações matriciais de R e S , tal como a seguir:

$$\begin{matrix} & R & & S & = & S \circ R \\ \begin{bmatrix} F & V & F \\ V & F & V \\ V & F & V \end{bmatrix} & & \begin{bmatrix} V & V \\ V & F \\ F & V \end{bmatrix} & & \begin{bmatrix} V & F \\ V & V \\ V & V \end{bmatrix} \end{matrix}$$

2.4 Equivalência e Congruência

Definição 2.13 Seja R uma relação em um conjunto A . R é:

Reflexiva Se para todo $x \in A$ $\langle x, x \rangle \in R$.

Simétrica Se para todo $x, y \in A$ se $\langle x, y \rangle \in R$ então $\langle y, x \rangle \in R$.

Transitiva Se para todo $x, y, z \in A$ se $\langle x, y \rangle \in R$ e $\langle y, z \rangle \in R$ então $\langle x, z \rangle \in R$.

Anti-simétrica Se para todo $x, y \in A$ se $\langle x, y \rangle \in R$ e $\langle y, x \rangle \in R$ então $x = y$.

Definição 2.14 Seja R uma relação em um conjunto A . Diz-se que R é uma relação de equivalência se R é reflexiva, simétrica e transitiva.

Exemplo 2.15

- A relação $=$ é o caso óbvio de relação de equivalência.
- A relação $R = \{\langle x, y \rangle \in \mathbb{N}^2 \mid \text{ter divisores comuns}\}$ não é uma relação de equivalência, R é evidentemente reflexiva e simétrica, mas não é transitiva, por exemplo $\langle 12, 15 \rangle \in R$, $\langle 15, 25 \rangle \in R$ porém $\langle 12, 25 \rangle \notin R$.
- A relação $R = \{\langle x, y \rangle \in \mathbb{N}^2 \mid \text{ter os mesmos divisores primos}\}$ é uma relação de equivalência.

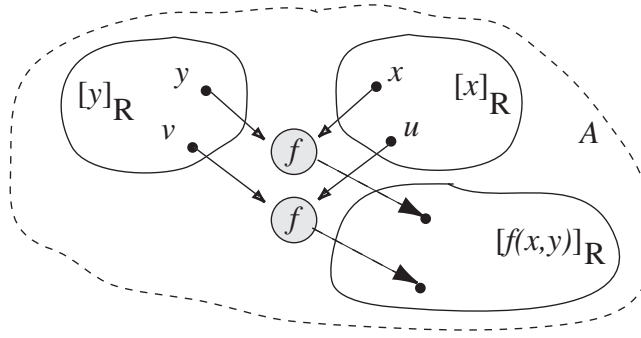


Figura 2.8: Partição em um conjunto A e f -congruência.

Definição 2.15 Seja R uma relação de equivalência (reflexiva, simétrica e transitiva) em um conjunto A e $x \in A$. Define-se a classe de equivalência de x com respeito a R por

$$[x]_R = \{y \in A \mid \langle x, y \rangle \in R\}$$

.

Lema 2.4 Seja R uma relação de equivalência em um conjunto A e $x \in A$. Então:

1. Se $\langle x, y \rangle \in R$ então $[x]_R = [y]_R$.
2. $[x]_R \cap [y]_R \neq \emptyset$ se e somente se $[x]_R = [y]_R$.
3. $\bigcup_{x \in A} [x]_R = A$

Definição 2.16 [Partição] Seja A um conjunto e $\{A_i\}_{i \in I}$ uma família de subconjuntos de A . Diz-se que $\{A_i\}_{i \in I}$ é uma partição de A se e somente se:

$$\bigcup_{i \in I} A_i = A \text{ e para todo } i, j \in I \text{ e } i \neq j \text{ } A_i \cap A_j = \emptyset$$

Lema 2.5 Seja R uma relação de equivalência em um conjunto A . A família de classes de equivalência de A com respeito a R $\{[x]_R\}_{x \in A}$ é uma partição de A .

Demonstração: É uma consequência do lema 2.4 e definição 2.16.

Definição 2.17 Seja A um conjunto, R uma relação de equivalência em A e $f : A^2 \rightarrow A$, diz-se que R é uma relação de congruência com respeito a f ou uma f -congruência se e somente se para todo $x, y, u, v \in A$ se $\langle x, u \rangle, \langle y, v \rangle \in R$ então $\langle f(x, y), f(u, v) \rangle \in R$. Ver Figura 2.8.

Exemplo 2.16 O conjunto \mathbb{N} pode ser partido pela relação \equiv_3 definida por $x \equiv_3 y \Leftrightarrow \text{resto}(x, 3) = \text{resto}(y, 3)$ onde $\text{resto}(x, y)$ é a função que nos fornece o resto da divisão de x por y . É fácil notar que \equiv_3 é uma relação de congruência com respeito a $+$.

2.5 Relações de Ordem

Definição 2.18 Diz-se que uma relação R em um conjunto A é uma relação de **ordem parcial** em A , ou simplesmente uma ordem em A se e somente se R é reflexiva, anti-simétrica e transitiva em A . A relação de ordem é dita ser **total** se e somente se para todo $x, y \in A$ $\langle x, y \rangle \in R$ ou $\langle y, x \rangle \in R$, se diz que esta ordem é linear. Relações de ordem parcial são em geral denotadas por \preceq (**precede**). Se $x \preceq y$ e $x \neq y$ dizemos que x **estritamente precede** y , o que denotamos por $x \prec y$.

Exemplo 2.17 As seguintes relações em \mathbb{N} são ordens parciais:

1. \geq é a mais conhecida das ordens parciais e é total.
2. xMy significando x é um múltiplo de y . Esta não é uma ordem total, por exemplo 3 não é múltiplo de 2 nem vice versa.

Definição 2.19 Uma estrutura de ordem ou simplesmente uma ordem é um par $\langle A, \preceq \rangle$, onde A é um conjunto e \preceq uma relação de ordem parcial em A .

Definição 2.20 Seja $\langle A, \preceq \rangle$ uma ordem e $X \subseteq A$. Diz-se que

1. $a \in A$ é um **limite inferior** de X se e somente se para todo $x \in X$, $a \preceq x$.
2. $a \in A$ é um **limite superior** de X se e somente se para todo $x \in X$, $x \preceq a$.

Referências Bibliográficas

- [1] HOPCROFT, J. E., *Theory os Machines and Compuatations*, chapter An n log n algorithm for minimizing states in a finite automaton, Academic Press, pp. 189–196, 1971.
- [2] MONTEIRO, A. A., PAULO, J. D. S., *Aritmética Racional*. Lisboa, Livraria Avelar Machado, 1945.
- [3] IFRAH, G., *Os Números: a história de uma grande invenção*. São Paulo, Globo S.A., 2005.
- [4] DEDEKIND, R., *Was sind und was sollen die Zahlen*, v. 3, *Gesammelte Mathematische Werke*. New York, Chelsea Publishing Company, 1969. pp. 335-391.
- [5] GÖDEL, K., *Collected Works*, v. 2, *Gesammelte Mathematische Werke*. Oxford, Oxford University Press, 1990.
- [6] ISRAEL, D., “Reflections on Gödel’s and Gandy’s Reflection on Turing’s Thesis”, *Minds and Machines*, v. 12, n. 2, pp. 181–201, 2002.
- [7] SOBRINHO, J. Z., “Aspectos da Tese de Church-Turing”, *Revista Matemática Universitária - USP*, v. 1, n. 6, pp. 1–23, 1987.
- [8] MCDERMOTT, D., “Artificial Intelligence Meets Natural Stupidity”, *SI-GART Newsletter*, v. 57, pp. 4–9, April 1976.
- [9] SETTI, M. D. O. G., *O Processo de Discretiza çã o do Raciocínio Matemático na Tradu çã o para o Raciocínio Computacional*, Report, Universidade Federal do Paraná, 2009.

- [10] GUERREIRO, G., “A Vanguarda Matemática e os Limites da Razão”, *Scientific American Brasil*, v. 5, n. 12, pp. 39–56, 2007. Coleção Gênios da Ciência.
- [11] SMULLYAN, R., *Gödel’s Incompleteness Theorems*. Oxford University Press, 1992.
- [12] GÖDEL, K., *The Undecidable*, chapter On Formally Undecidable Propositions of Principia Mathematica and Related Systems, New York, Raven Press, pp. 5–38, 1965.
- [13] WHITEHEAD, A. N., RUSSELL, B., *Principia Mathematica*. Londres, Cambridge University Press, 1913.
- [14] NAGEL, E., NEWMAN, J. R., *Gödel’s Proof*. USA, Routledge, 1989.
- [15] GÖDEL, K., “Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme - On Formally Undecidable Propositions of Principia Mathematica and Related Systems”, *Kurt Gödel: Collected Works*, v. 1, n. 1, pp. 144–195, 1986. Tradução para o inglês por Martin Hirzel. www.research.ibm.com/people/h/hirzel/papers/canon00-goedel.pdf [capturado em 13 de agosto de 2011].
- [16] MELO, A. C. V. D., SILVA, F. S. C. D., *Modelos Clássicos de Computação*, Coleção Schaum. São Paulo, Thomson, 2006.
- [17] KUBRUSLY, R. D. S., *Uma viagem informal ao Teorema de Gödel ou (O preço da matemática é o eterno matemático)*, Report, Universidade Federal do Rio de Janeiro, 2007. IM/UFRJ.
- [18] SMULLYAN, R., *Recursion Theory for Metamathematics*. Oxford University Press, 1993.
- [19] SMULLYAN, R., *What’s the Name of This Book*. Penguin Books, 1978.
- [20] SMULLYAN, R., *Forever Undecided: A Puzzle Guide to Gödel*. Oxford University Press, 1987.
- [21] GOLDSTEIN, R., *Incompleteness: The Proof and Paradox of Kurt Gödel*. W. W. Norton Company, Inc., 2005.

- [22] HOFSTADTER, D. R., *Gödel, Escher e Bach: an Eternal Golden Braid*. Nova Iorque, Basic Books, 1979.
- [23] Rodríguez-Consuegra, F. A. (ed.), *Kurt Gödel - Unpublished Philosophical Essays*. Berlin, Birkhäuser Verlag, 1995.
- [24] Feferman, S., *et al.* (eds.), *Kurt Gödel - Collected Works*, v. I, II, III. New York, Oxford University Press, 1986.
- [25] WANG, H., *Reflections on Kurt Gödel*. Cambridge, Massachusetts, The MIT Press, 1988.
- [26] SUPPES, P., *Axiomatic Set Theory*. New York, Dover, 1972.
- [27] LIPSCHUTZ, S., *Teoria Elementar dos Conjuntos*, Cole çã o Schaum. Sã o Paulo, McGraw-Hill do Brasil, 1990.
- [28] SUPPES, P., *Axiomatic Theory Set*. USA, Van Nostrand Company Inc., 1960.
- [29] MELLO, F. L. D., CARVALHO, R. L. D., “Knowledge Geometry”, *Journal of Information and Knowledge Management*, v. 14, pp. 1550028, 2015.
- [30] STOLL, R. R., *Set Theory and Logic*. USA, Dover Publications Inc., 1961.
- [31] MIRAGLIA, F., *Teoria dos Conjuntos: um mínimo*. Brasil, Edusp - Editora da Universidade de São Paulo, 1992.
- [32] HALMOS, P., *Teoria Ingênua dos Conjuntos*. Brasil, Edusp - Editora da Universidade de São Paulo, 1970.
- [33] GRATZER, G., *Universal Algebra*. USA, Van Nostrand Company Inc., 1968.
- [34] COHN, P. M., *Universal Algebra*. USA, Harper and Row, 1965.
- [35] GALLIER, J. H., *Logic for Computer Science*. USA, John Wiley and Sons Inc., 1987.
- [36] PREPARATTA, F. P., YEH, R. T., *Introduction to Discrete Structures for Computer Science and Engineering*. USA, Addison-Wesley Publishing Company, 1973.

- [37] SHOENFIELD, J. R., *Degrees of Unsolvability*. North-Holland Publishing Company, 1971.
- [38] BRAINERD, W. S., LANDWEBER, L. H., *Theory of Computation*. USA, John Wiley and Sons, 1974.
- [39] EILENBERG, S., ELGOT, C., *Recursiveness*. New York: Academic Press, 1970.
- [40] CARVALHO, R. L. D., OLIVEIRA, C. M. G. M. D., *Modelos de Computação e Sistemas Formais*, 11^a Escola de Computação. Rio de Janeiro, Universidade Federal do Rio de Janeiro, 1998.
- [41] BRAINERD, W. S., LANDWEBER, L. H., *Theory of Computation*. John Wiley & Sons, 1974.
- [42] KLEENE, S. C., *Introduction to Metamathematics*. D. Van Nostrand Company, Inc., 1952.
- [43] Rogers Jr., H., *Theory of Recursive Functions and Effective Computability*. USA, McGraw-Hill Book Company, 1967.
- [44] DAVIS, M., *Computability and Unsolvability*. New York, Dover, 1983.
- [45] BOOLOS, G. S., JEFFREY, R. C., *Computability and Logic*. Cambridge University Press, 1974.
- [46] MARTIN DAVIS, R. S., WEYUKER, E. J., *Computability Complexity and Languages*. New York, Academic Press, 1994.
- [47] MALLOZZI, J. S., LILLO, N. J. D., *Computability with Pascal*. New Jersey, Prentice-Hall, Inc., 1984.
- [48] TURING, A. M., *The Undecidable*, chapter On Computable Numbers, with an Application to the Entscheidungsproblem, New York, Raven Press, pp. 115–151, 1965.
- [49] ELGOT, C. C., ROBINSON, A., “Random-access stored-program machines, an approach to programming languages”, *Journal of the ACM*, v. 11, pp. 365–399, 1964.

- [50] PREPARATTA, F. P., YEH, R. T., *Introduction to Discrete Structures for Computer Science and Engineering*. Addison-Wesley Publishing Company, 1973.
- [51] HENNIE, F., *Introduction to Computability*. Addison-Wesley Publishing Company, 1977.
- [52] NELSON, R. J., *Introduction to Automata*. USA, Jonh Wiley & Sons, Inc., 1968.
- [53] CARVALHO, R. L. D., *Máquinas, Programas e Algoritmos*, 2^a Escola de Computação. Campinas, Universidade Estadual de Campinas, 1981.
- [54] MENDELSON, E., *Introduction to Mathematical Logic*, Cole Mathematics Series. 3 ed. The Wadsworth and Brooks, 1987.
- [55] MANIN, Y. I., *A Course in Mathematical Logic*, Graduate Texts in Mathematics 53. 1 ed. Springer-Verlag, 1977.
- [56] HOMER, S., SELMAN, A. L., *Computability and Complexity Theory*, Texts in Computer Science. 2 ed. Springer, 2011.
- [57] CUTLAND, N. J., *Computability: An introduction to recursive function theory*. Cambridge University Press, 1980.
- [58] SIPSER, M., *Introduction to The Theory of Computation*, Course Technology Series. 2 ed. Thomson, 2006.
- [59] WALTER CARNIELLI, R. L. E., *Computability: computable functions, logic and the foundations of mathematics*. Belmont, Wadsworth and Brooks, 1989.
- [60] TARSKI, A., *Logic, semantics, metamathematics*, chapter Fundamental concepts of the methodology of the deductive sciences, London, Oxford at the Clarendon Press, pp. 60–109, 1969.
- [61] ADAM YOUNG, M. Y., *Malicious Cryptography: Exposing Cryptovirology*. John Wiley and Sons Inc., 2004.

- [62] BONFANTE, G., KACZMAREK, M., MARION, J.-Y., *A Classification of Viruses through Recursion Theorems*, volume 4497 of Lecture Notes in Computer Science. 2 ed. CiE 2007, 2007.
- [63] MACHTEY, M., YOUNG, P., *An Introduction to the General Theory of Algorithms*. New York, North Holland, 1978.
- [64] ROBINSON, J. A., “A machine oriented logic based on the resolution principle”, *J. Assoc. Comput.*, v. 12, pp. 23–41, 1965.
- [65] ROBINSON, J. A., “Automatic deduction with hyper-resolution”, *Internat. J. Comput. Math.*, v. 1, pp. 227–234, 1965.
- [66] GILMORE, P. C., “A proof method for quantification theory: Its justification and realization”, *IBM Journal of Research and Development*, v. 4, n. 1, pp. 28–35, 1960.
- [67] DAVIS, M., PUTNAM, H., “A computing procedure for quantification theory”, *Journal of the ACM*, v. 7, n. 3, pp. 201–215, 1960.
- [68] CHANG, C.-L., LEE, R. C.-T., *Symbolic Logic and Mechanical Theorem Proving*. Academic Press Inc, 1973.
- [69] KLEENE, S. C., *Mathematical Logic*. Wiley, 1967.
- [70] HILBERT, D., ACKERMANN, W., *Prinmciples of Mathematical Logic*. Chelsea, 1950.
- [71] MCCAWLEY, J. D., *Everything That Linguists Have Always Wanted To Know About Logic*. 2 ed. The University of Chicago Press, 1993.
- [72] SUPPES, P., *Introduction to Logic*. D. van Nostrand, 1966.
- [73] RUSSELL, B., *A Filosofia do Atomismo Lógico*, *Lógica e Conhecimento*. 1 ed. Abril Cultural, 1974. (Os Pensadores, 42).
- [74] RUSSELL, B., *Significado e Verdade*. 1 ed. Zahar, 1978.
- [75] POPPER, K. R., *A Lógica da Pesquisa Científica*. 2 ed. Cultrix, 1974.

- [76] LAKATOS, I., , MUSGRAVE, A., *A Crítica e o Desenvolvimento do Conhecimento*. 1 ed. EDUSP, Cultrix, 1979. Tradução: M. O. Caiado.
- [77] WANG, H., *From Mathematics to Philosophy*. 1 ed. Cultrix, 1974.
- [78] GREEN, C. C., *The Application of Theorem Proving to Question-Answering Systems*. Ph.D. dissertation, Stanford, June 1969. AI Project MEMO AI-96.
- [79] LOVELAND, D. W., *Automated Theorem Proving: a Logical Basis*. 1 ed. North Holland, 1978.
- [80] HUGHES, G. E., LONDEY, D. G., *The Elements of Formal Logic*. USA, Methuen and Co Ltd, 1965.
- [81] BOOK, R. V., OTTO, F., *String-Rewriting Systems*. USA, Springer-Verlag, 1993.
- [82] HOPCROFT, J. E., ULLMAN, J. D., *Introduction to Automata Theory, Language and Computation*. USA, Addison-Wesley Publishing Company, 1979.
- [83] HOPCROFT, J. E., ULLMAN, J. D., *Formal Languages and their Relation to Automata*. USA, Addison-Wesley Publishing Company, 1969.
- [84] CURRY, H. B., *Foundations of Mathematical Logic*. New York, Academic Press, 1977.
- [85] SMULLYAN, R., *Theory of Formal Systems*. USA, Princeton, 1961.
- [86] BERSTEL, J., BOASSON, L., CARTON, O., *et al.*, *Handbook of Automata: from Mathematics to Applications*, chapter Minimization of automata, European Mathematical Society, pp. 189–196, 2010.
- [87] BEAL, M. P., CROCHEMORE, M., “Minimizing incomplete automata”, *Workshop on Finite State Methods and Natural Language Processing*, , september 2008. Ispra.
- [88] VALMARI, A., LEHTINEN, P., “Efficient minimization of DFAs with partial transition”, *Proc. 25th Symp. Theoretical Aspects of Comp. Sci.*, v. 08001, pp. 645–656, 2008. S. Albers and P. Weil, editors.

- [89] PAPADONIKOLAKIS, M., BOUGANIS, C.-S., CONSTANTINIDES, G.,
“Performance comparison of GPU and FPGA architectures for the SVM training problem”, *IEEE International Conference on FieldProgrammable Technology*, pp. 388–391, 2009.
- [90] MU, S., WANG, C., LIU, M., *et al.*, “Evaluating the potential of graphics processors for high performance embedded computing”, *Proc. IEEE Design, Automation and Test in Europe Conference and Exhibition*, pp. 709–714, 2011.
- [91] KAI HWANG, F. A. B., *Computer Architecture and Parallel Processing*. McGraw-Hill, 1984.
- [92] AGARWAL, P., KRISHNAN, S., MUSTAFA, N., *et al.*, *Algorithms - ESA 2003, Lecture Notes in Computer Science*, chapter Streaming Geometric Optimization Using Graphics Hardware, Springer Berlin-Heidelberg, pp. 115–151, 2003.
- [93] TANENBAUM, A. S., *Organização Estruturada de Computadores*. 3 ed. Prentice Hall do Brasil, 1997.
- [94] BACKUS, J., “Can Programming be Liberated from von Neumann Style? A functional style and its algebra of program”, *ACM Turing Award Lecture, Communications of the ACM*, v. 21, n. 8, pp. 613–641, 1978.
- [95] OWENS, J. D., LUEBKE, D., GOVINDARAJU, N., *et al.*, “A Survey of General-Purpose Computing on Graphics Hardware”, *Eurographics 2005, State of the Art Reports*, pp. 21–51, 2005.
- [96] GUSTAFSON, J. L., “Reevaluating Amdahl’s law”, *Communications of the ACM*, v. 5, n. 31, pp. 532, 1988.
- [97] HANDLER, W., *Parallel Processing Systems, an advanced course*, chapter Innovative computer architecture - how to increase parallelism but not complexity, Cambridge University Press, pp. 1–41, 1982.
- [98] LOBUR, J., NULL, L., *The Essentials of Computer Organization And Architecture*. Jones and Bartlett Pub, 2006.

- [99] LEWIS, H. R., PAPADIMITRIOU, C. H., *Elements of the Theory of Computation*. 2 ed. New York, Prentice-Hall, 1998.
- [100] DUNNE, P., *Computability Theory: Concepts and Applications*. Ellis Horwood, 1991.
- [101] AARONSON, S., “NP-complete Problems and Physical Reality”, *ACM SIGACT News*, , march 2005. Complexity Theory Column 46.