Capítulo 2

Fundamentos Matemáticos

Neste capítulo, introduziremos a base matemática necessária para a compreensão da pesquisa desenvolvida nesta tese. Na Seção 2.1, recordaremos algumas definições e propriedades da teoria de conjuntos. Na Seção 2.2, veremos algumas definições da teoria dos grupos.

Assumiremos aqui que o leitor tenha alguma familialidade com conceitos básicos da Teoria da Complexidade Computacional, razão pela qual não incluímos nenhuma seção sobre tais conceitos. Ademais, a terminologia utilizada segue exatamente a de Garey e Johnson [21].

As definições e conceitos que apresentamos neste capítulo não pretendem abranger toda a teoria, mas apenas introduzir os elementos necessários para a compreensão do texto nos capítulos seguintes. Desta forma, somente algumas propriedades serão demonstradas; as provas das propriedades e dos resultados mencionados neste capítulo que possam ser encontradas nas referências citadas não serão apresentadas.

O conteúdo deste capítulo pode ser facilmente compreendido e não é nenhum obstáculo para a leitura desta tese, pois em sua maioria as definições e propriedades são bastante conhecidas na literatura. No entanto, aconselhamos uma rápida leitura do mesmo com o objetivo de se familiarizar com as notações e nomenclaturas utilizadas nos capítulos posteriores.

2.1 Teoria dos Conjuntos

Nesta seção, recordaremos algumas propriedades e alguns conceitos básicos da teoria dos conjuntos [17] que serão utilizados ao longo desta tese. Na Subseção 2.1.1, apresentamos as noções fundamentais de conjunto. Na Subseção 2.1.2, apresentamos a notação utilizada nesta tese para o conjunto dos números inteiros. Na Subseção 2.1.3, definimos algumas operações com conjuntos e mostramos algumas de suas propriedades. Na Subseção 2.1.4, definimos o produto cartesiano entre dois ou mais conjuntos. Na Subseção 2.1.5, definimos alguns tipos de relações entre conjuntos. Na Subseção 2.1.6, definimos o que são as classes de equivalência de um conjunto e apresentamos algumas de suas propriedades. Na Subseção 2.1.7, definimos o que é uma partição de um conjunto. Finalmente, na Subseção 2.1.8, definimos o que vem a ser uma função.

2.1.1 Noções Fundamentais de Conjunto

Um *conjunto* A é uma coleção de elementos de um determinado universo, denotado genericamente por U. Se um elemento x do universo U *pertence* ao conjunto A, então escrevemos $x \in A$ (leia-se, x pertence a A); caso contrário, $x \notin A$.

Um *conjunto finito* é um conjunto com um número finito de elementos. Um conjunto que não é finito diz-se *infinito*. Salvo indicação contrária, usaremos o termo "conjunto" significando "conjunto finito". A *cardinalidade* de um conjunto finito A, denotada por $|A|$, é o número de elementos pertencentes a A.

Um *conjunto vazio*, denotado por $\emptyset$, é um conjunto que não contém nenhum elemento. Um conjunto unitário é um conjunto constituído por um único elemento.

Um conjunto A está *contido* em um outro conjunto B se, e somente se, todo elemento de A pertence a B, isto é, $A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B)$. Neste caso, diz-se que A é um *subconjunto* de B.

Dizemos que um conjunto A é um *superconjunto* de um outro conjunto B se, e somente se, B é um subconjunto de A, isto é, $A \supseteq B \Leftrightarrow B \subseteq A$.

Um conjunto A está *propriamente contido* em um outro conjunto B se, e somente se, A está contido em B e A é diferente de B, isto é, $A \subset B \Leftrightarrow (A \subseteq B$ e $A \neq B)$. Neste caso, diz-se que A é um *subconjunto próprio* de B.

Dizemos que um conjunto A é *igual* a um outro conjunto B se, e somente se, $A \subseteq B$ e $B \subseteq A$.

A proposição seguinte é um consequência imediata da relação de inclusão entre conjuntos.

Proposição 2.1 *Sejam A e B dois conjuntos. Se $A \subseteq B$ e $A \neq B$, então $|A| < |B|$.*

O *conjunto das partes* de um conjunto E, denotado por $\mathcal{P}(E)$, é o conjunto cujos elementos são todos os subconjuntos de E, isto é, $\mathcal{P}(E) = \{X : X \subseteq E\}$. Note que $\emptyset \in \mathcal{P}(E)$, $E \in \mathcal{P}(E)$ e se $|E| = n$, então $|\mathcal{P}(E)| = 2^n$.

2.1.2 Conjunto dos Números Inteiros

Ao longo deste texto, denotaremos o conjunto dos números inteiros por $\mathbb{Z}$. Dizemos que um número inteiro x é *não negativo* se, e somente se, $x \geq 0$. O conjunto de todos os inteiros não negativos é denotado por $\mathbb{Z}_+$. Um número inteiro x é dito *positivo* se, e somente se, $x > 0$. Denotaremos o conjunto dos números inteiros positivos por $\mathbb{Z}_+^*$.

2.1.3 Operações com Conjuntos

Nesta subseção apresentaremos três operações básicas com conjuntos: complemento, intersecção e união.

Sejam A e E dois conjuntos tais que $A \subseteq E$. O *complemento* de A em relação a E é o conjunto de todos os elementos de E que não pertencem a A, isto é, $A_E^c = \{x \in E : x \notin A\}$. Quando o conjunto E está claramente definido pelo contexto, escreveremos simplesmente A^c.

A seguinte proposição [17, p. 48] apresenta duas propriedades da operação complemento.

Proposição 2.2 *Sejam A, B e E três conjuntos tais que $A, B \subseteq E$. Então valem as seguintes propriedades do complemento em relação a E.*

(a) $(A^c)^c = A$;
(b) $A \subseteq B \Rightarrow B^c \subseteq A^c$.

A *intersecção* de dois conjuntos A e B é o conjunto de todos os elementos que pertencem simultanemente a A e a B, isto é, $A \cap B = \{x : x \in A \text{ e } x \in B\}$.

A *intersecção* de n conjuntos $A_1, A_2, \cdots, A_n$ é o conjunto de todos elementos que pertencem simultaneamente a todos estes n conjuntos, isto é, $\cap_{i=1}^n A_i = \{x : x \in A_1 \text{ e } x \in A_2 \text{ e } \cdots \text{ e } x \in A_n\}$.

Dizemos que dois conjuntos A e B são *disjuntos* se, e somente se, $A \cap B = \emptyset$.

A *união* de dois conjuntos A e B é o conjunto de todos os elementos que pertencem a A ou a B, isto é, $A \cup B = \{x : x \in A \text{ ou } x \in B\}$.

A *união* de n conjuntos $A_1, A_2, \cdots, A_n$ é o conjunto de todos elementos que pertencem a pelo menos um destes n conjuntos, isto é, $\cup_{i=1}^n A_i = \{x : x \in A_1 \text{ ou } x \in A_2 \text{ ou } \cdots \text{ ou } x \in A_n\}$.

A seguir apresentamos algumas propriedades da intersecção e da união entre conjuntos. As demonstrações destas propriedades podem ser encontradas em [17].

Proposição 2.3 *Seja U o conjunto universo. Se $A, B, C \subseteq U$, então valem as seguintes propriedades.*

(a) $A \cap B \subseteq A$ *e* $A \cap B \subseteq B$	(b) $A \subseteq A \cup B$ *e* $B \subseteq A \cup B$
(c) $A \subseteq B \Leftrightarrow A \cap B = A$	(d) $A \subseteq B \Leftrightarrow A \cup B = B$
(e) $A \subseteq B \Rightarrow A \cap C \subseteq B \cap C$	(f) $A \subseteq B \Rightarrow A \cup C \subseteq B \cup C$
(g) $A \subseteq B$ *e* $A \subseteq C \Rightarrow A \subseteq B \cap C$	(h) $A \subseteq B$ *e* $A \subseteq C \Rightarrow A \subseteq B \cup C$
(i) $A \subseteq C$ *e* $B \subseteq C \Rightarrow A \cap B \subseteq C$	(j) $A \subseteq C$ *e* $B \subseteq C \Rightarrow A \cup B \subseteq C$
(k) $A \cap B = B \cap A$	(l) $A \cup B = B \cup A$
(m) $(A \cap B) \cap C = A \cap (B \cap C)$	(n) $(A \cup B) \cup C = A \cup (B \cup C)$
(o) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(p) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(q) $x \in A \cap B \Leftrightarrow x \in A$ *e* $x \in B$	(r) $x \in A \cup B \Leftrightarrow x \in A$ *ou* $x \in B$

Os dois resultados seguintes (Proposições 2.4 e 2.5) são conseqüências das propriedades distributivas da intersecção e união dadas nas Proposições 2.3.o e 2.3.p.

Proposição 2.4 *Sejam* $A, X, Y \in \mathcal{P}(E)$ *tais que se* $A \subseteq X \subseteq Y$*, então* $(A \cup X_Y^c) \cap X = A$.

Prova:

$$\begin{aligned} (A \cup X^c) \cap X &= (A \cap X) \cup (X^c \cap X) && \text{(pela Proposição 2.3.}o\text{)} \\ &= A && \text{(uma vez que } A \subseteq X\text{).} \end{aligned}$$

∎

Proposição 2.5 *Sejam* $A, X, Y \in \mathcal{P}(E)$ *tais que* $X \subseteq Y$ *e* $A \subseteq Y$*. Se* $A - X = X_Y^c$*, então* $(A \cap X) \cup X_Y^c = A$.

Prova: Primeiramente, provaremos que $A - X = X_Y^c \Leftrightarrow X_Y^c \subseteq A$ da seguinte forma.

$$\begin{aligned} A - X = X_Y^c &\Leftrightarrow A \cap X_Y^c = X_Y^c \\ &\Leftrightarrow X_Y^c \subseteq A. \end{aligned}$$

Finalmente, $(A \cap X) \cup X_Y^c = A$, uma vez que

$$\begin{aligned} (A \cap X) \cup X_Y^c &= (A \cup X_Y^c) \cap (X \cup X_Y^c) && \text{(pela Proposição 2.3.}p\text{)} \\ &= A \cap Y && \text{(uma vez que } X_Y^c \subseteq A\text{)} \\ &= A && \text{(uma vez que } A \subseteq Y\text{).} \end{aligned}$$

∎

2.1.4 Produto Cartesiano

Sejam A e B dois conjuntos. Dados $x \in A$ e $y \in B$, dizemos que (x, y) é, ou forma, um *par ordenado*. Dizemos que o elemento x é a *primeira coordenada* e que o elemento y é a *segunda coordenada* do par ordenado (x, y).

Generalizando, dados n conjuntos $A_1, A_2, \cdots, A_n$ e elementos $x_i \in A_i$, para $i \in \{1, 2, \cdots, n\}$, dizemos que $(x_1, x_2, \cdots, x_n)$ é, ou forma, uma *n-upla ordenada*. Cada elemento x_i, $i \in \{1, 2, \cdots, n\}$, é a i-ésima coordenada da n-upla $(x_1, x_2, \cdots, x_n)$.

Sejam A e B dois conjuntos. O *produto cartesiano* de A por B, denotado por $A \times B$, é o conjunto formado por todos pares ordenados (x, y), tais que $x \in A$ e $y \in B$, isto é, $A \times B = \{(x, y) : x \in A,\ y \in B\}$. O *quadrado de um conjunto* A é o produto cartesiano de A por A, isto é, $A^2 = A \times A$.

Generalizando, o *produto cartesiano de n conjuntos* $A_1, A_2, \cdots, A_n$, denotado por $A_1 \times A_2 \times \cdots \times A_n$, é o conjunto formado por todas n-uplas ordenadas $(x_1, x_2, \cdots, x_n)$, onde $x_i \in A_i$, $i \in \{1, 2, \cdots, n\}$, isto é, $A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \cdots, x_n) : x_1 \in A_1,\ x_2 \in A_2,\ \cdots,\ x_n \in A_n\}$. No caso particular em que $A = A_1 = A_2 = \cdots = A_n$, $A^n = A_1 \times A_2 \times \cdots \times A_n$ é a *n-ésima potência* de A.

2.1.5 Relações sobre Conjuntos

Uma *relação binária* R de um conjunto A com um conjunto B é uma terna ordenada $R = (G, A, B)$, onde $G \subseteq A \times B$. Dizemos que x está relacionado com y pela relação R se, e somente se, $(x, y) \in G$, isto é, $xRy \Leftrightarrow (x, y) \in G$.

Quando $B = A$, dizemos simplesmente que R é uma relação sobre A.

A *inversa* de uma relação binária R de um conjunto A com um conjunto B é a relação binária R^{-1} de B com A definida como, para todo $x \in A$ e $y \in B$, $yR^{-1}x \Leftrightarrow xRy$.

Uma relação binária R sobre um conjunto A é dita *reflexiva* se, e somente se, para todo $x \in A$, temos que xRx.

Uma relação binária R sobre um conjunto A é dita *simétrica* se, e somente se, para todo $x, y \in A$, temos que $xRy \Rightarrow yRx$.

Uma relação binária R sobre um conjunto A é dita *anti-simétrica* se, e somente se, para todo $x, y \in A$, temos que xRy e $yRx \Rightarrow x = y$.

Uma relação binária R sobre um conjunto A é dita *transitiva* se, e somente se, para todo $x, y, z \in A$, temos que xRy e $yRz \Rightarrow xRz$.

Uma relação binária R sobre um conjunto A é uma *relação de equivalência* se, e somente se, ela é reflexiva, simétrica e transitiva.

2.1.6 Classes de Equivalência

Sejam A um conjunto e R uma relação de equivalência sobre A. Se $x, y \in A$ são tais que xRy, então dizemos que x é equivalente a y segundo R e denotaremos $x \equiv_R y$. Quando a relação de equivalência está claramente definida pelo contexto, escreveremos simplesmente $x \equiv y$.

Seja A um conjunto não vazio. Sejam R uma relação de equivalência sobre A e $x \in A$. A *classe de equivalência* segundo R do elemento x é o conjunto de todos os elementos de A que são equivalentes a x segundo R, isto é, $\mathcal{C}_R(x) = \{y \in A : y \equiv_R x\}$. Quando a relação de equivalência está claramente definida pelo contexto, escreveremos simplesmente $\mathcal{C}(x)$.

Note que, para todo $x \in A$, $x \in \mathcal{C}_R(x)$, pois pela propriedade reflexiva de R, xRx. Logo, $\mathcal{C}_R(x)$ nunca é vazia, isto é, $\mathcal{C}_R(x) \neq \emptyset$.

Seja A um conjunto não vazio. Sejam R uma relação de equivalência sobre A e $x \in A$. Dizemos que a classe de equivalência $\mathcal{C}_R(x)$ é *determinada* ou *definida* pelo elemento x, o qual por sua vez, é o *representante* de $\mathcal{C}_R(x)$.

A seguinte proposição [17, p. 163] é uma propriedade de classes de equivalência.

Proposição 2.6 *Seja R uma relação de equivalência em um conjunto não vazio A e sejam $x, y \in A$. Então valem as seguintes propriedades:*

(*a*) $\mathcal{C}_R(x) = \mathcal{C}_R(y) \Leftrightarrow x \equiv_R y$;
(*a*) *se* $\mathcal{C}_R(x) \cap \mathcal{C}_R(y) \neq \emptyset$, *então* $\mathcal{C}_R(x) = \mathcal{C}_R(y)$.

Seja R uma relação de equivalência em um conjunto não vazio A e sejam $x, y \in A$. Pela Proposição 2.6a, temos que se $y \in \mathcal{C}_R(x)$, então $\mathcal{C}_R(x) = \mathcal{C}_R(y)$. Portanto, qualquer elemento de $\mathcal{C}_R(x)$ é um representante de $\mathcal{C}_R(x)$.

Sejam A um conjunto não vazio e R uma relação de equivalência sobre A. O *conjunto quociente* de A pela relação de equivalência R é o conjunto formado por todas as classes de equivalência segundo R, isto é, $\mathcal{Q}_R(A) = \{\mathcal{C}_R(x) : x \in A\}$. Quando a relação de equivalência está claramente definida pelo contexto, escreveremos simplesmente $\mathcal{Q}(A)$.

Denotaremos por $\mathcal{R}_R(A)$, ou simplesmente $\mathcal{R}(A)$ quando a relação de equivalência está claramente definida pelo contexto, o conjunto formado por exatamente um representante de cada classe de equivalência de $\mathcal{Q}_R(A)$, isto é, $\mathcal{R}_R(A)$ é um conjunto tal que $|\mathcal{R}_R(A)| = |\mathcal{Q}_R(A)|$.

2.1.7 Partição de um Conjunto

Seja A um conjunto não vazio. Uma partição de A é um conjunto $\mathsf{P}(A)$ de partes não vazias de A, disjuntas duas a duas e cuja união é A, isto é, $\mathsf{P}(A) \subseteq \mathcal{P}(A)$ que satisfaz as três seguintes condições:

(*a*) se $X \in \mathsf{P}(A)$, então $X \neq \emptyset$;
(*b*) se $X_i, X_j \in \mathsf{P}(A)$ e $X_i \neq X_j$, então $X_i \cap X_j = \emptyset$;
(*c*) $\cup\{X : X \in \mathsf{P}(A)\} = A$.

A seguinte proposição [17, p. 165] afirma que uma relação de equivalência sobre um conjunto A define uma partição de A.

Proposição 2.7 *Dados um conjunto não vazio A e uma relação de equivalência R em A, o conjunto quociente $\mathcal{Q}_R(A)$ é uma partição de A.*

2.1.8 Funções

Uma *função* (ou *mapeamento* ou *transformação*) de um conjunto A em um outro conjunto B é uma relação binária $f = (F, A, B)$ de A com B que satisfaz as seguintes condições:

(1) $\forall x \in A, \exists y \in B : (x, y) \in F$;
(2) $\forall x \in A$, se $(x, y), (x, z) \in F$, então $y = z$;

Uma função f de A em B é indicada por $f : A \to B$. Para cada elemento $x \in A$, o único elemento $y \in B$ tal que $(x, y) \in F$ é chamado *imagem* de x pela função f ou *valor* da função f em x e é denotado por $y = f(x)$.

Dada uma função $f : A \to B$, os conjuntos A e B são chamados de *domínio* e *contradomínio* da função f. O conjunto $\{f(x) : x \in A\} \subseteq B$ é chamado *imagem* da função f e é denotado por $f(A)$.

Uma função $f : A \to B$ é *sobrejetora* se, e somente se, para todo $y \in B$, existe um $x \in A$ tal que $f(x) = y$, isto é, $\forall y \in B, \exists x \in A : f(x) = y$.

Uma função $f : A \to B$ é *injetora* se, e somente se, para quaisquer dois elementos distintos $x_1, x_2 \in A$, temos imagens distintas $f(x_1), f(x_2) \in B$, isto é, se $x_1, x_2 \in A$ e $x_1 \neq x_2$, então $f(x_1) \neq f(x_2)$.

Uma função $f : A \to B$ é *bijetora* se, e somente se, ela é sobrejetora e injetora ao mesmo tempo.

Dada uma função $f : A \to B$, a relação inversa f^{-1} de B com A (isto é, $f^{-1} = (F^{-1}, B, A)$ onde $F^{-1} = \{(y, x) : (x, y) \in F\}$), é uma função se, e somente se, f é uma função bijetora. A função f^{-1}, se existe, é chamada *função inversa* de f.

Sejam $f : A \to B$ e $g : B \to C$. Definimos a *composição* da função f com a função g a função $g \cdot f : A \to C$ como $g \cdot f(x) = g(f(x))$, para todo $x \in A$. A função $g \cdot f$ é também chamada de *função composta* de g e f. Em geral denotamos $g \cdot f$ simplesmente por gf ou $g(f)$.

A seguir, definimos uma função bastante conhecida e muito utilizada nesta tese. A função $\lceil \cdot \rceil$, definida do conjunto dos números reais no conjunto dos números inteiros, é chamada de *função teto* e ela é definida da seguinte forma: se x é um número real qualquer, então $\lceil x \rceil$ corresponde ao menor inteiro maior ou igual a x. Por exemplo, se $y = 2.7182$, então $\lceil x \rceil = 3$ e $\lceil -x \rceil = -2$.

2.2 Teoria dos Grupos

Um conjunto G, munido com uma operação binária $+$ é um *grupo*, se satisfaz os seguintes axiomas:

(a) $a + (b + c) = (a + b) + c, \quad \forall\ a, b, c \in G$;

(b) G contém um elemento e tal que $e + a = a + e = a$, para todo $a \in G$;

(c) $\forall\ a \in G$, existe um elemento em G, denotado por $-a$, tal que $a + (-a) = (-a) + a = e$.

Um grupo G munido com uma operação binária $+$ será denotado por $(G, +)$. O elemento e que satisfaz a condição (b) é chamado de elemento neutro de $(G, +)$.

Um grupo $(G, +)$ é chamado de *grupo abeliano* se, e somente se, para quaisquer $a, b \in G$, $a + b = b + a$.