MATEMÁTICA E COMPUTAÇÃO FORMAL

Prof. Valdigleis S. Costa

Valdigleis S. Costa
Professor Adjunto, Colegiado de Ciência da Computação
Universidade Federal do Vale do São Francisco
Salgueiro, PE

Página pessoal do autor https://valdigleis.site

Este tomo foi escrito com base em uma coleção de notas de aulas do autor, o mesmo foi redigido usando um *template* desenvolvido pelo próprio autor. Este texto foi escrito com o conjunto de macros LaTeX (em sua versão 2) e compilado usado as ferramentas LuaLaTeX e BibTeX, tais ferramentas fornecidas pelas distribuições TeXLive e MacTeX, respectivamente nos sistema operacionais *Unix-like*: Gnu/Linux (Debian) e no Mac OS X, para edição foi usando o *software* livre de edição textual Vim (versão 9.0.1499) e o sistema de controle de versão adotado é o Git.

Release compilado em 25 de junho de 2024–10:44:00.

Sobre este documento

Este documento vem sendo construído aos poucos (em passos de tartaruga), tendo como base diversas notas de aula (manuscritas a mão) que eu preparei para ministrar cursos de graduação nos seguintes tópicos:

(i) Conjuntos, relações e funções;
(ii) Lógica;
(iii) Álgebra universal;
(iv) Teoria dos códigos;
(v) Linguagem formais e autômatos;
(vi) Computabilidade e decidibilidade;
(vii) Análise de algoritmos;
(viii) Grafos;
(ix) Categorias;
(x) Teoria da Informação;

Uma vez que este documento ainda é um projeto em andamento e possivelmente sua escrita nunca será realmente concluída com total aprovação de seu autor, é claro que você poderá encontrar diversos erros, que com toda certeza você leitor irá me enviar e-mails[1] ou *issues*[2] com reports de tais erros, no caso de ser meu aluno também pode fazer apontamentos através da comunidade **extra-classe**[3]. Para acessar a página da nova versão deste documento basta escanear o ***QR code*** abaixo.

Sobre os questionários encontrados neste documento tem-se que, as questões apresentam-se de dois tipos, primeiro as questões sem resposta pronta, e as questões cuja resposta pode ser encontradas no caderno de respostas.

Para finalizar, a personagem que você irá encontrar de forma recorrente neste documento chama-se ALiCIA[4], ela é uma criação do autor deste livro e todas as imagens da mesma são de propriedade do autor, não sendo permitido o usado das imagens por terceiros sem autorização assinada pelo autor deste documento.

---

[1] E-mail do autor: `valdigleis@gmail.com`
[2] Páginas de *issues*: `https://gitlab.com/valdigleis/mcf/-/issues`
[3] Acessível através do link `https://valdigleis.site/extraclasse`
[4] ALiCIA é um acrônimo para Autômatos, Linguagens, Complexidade, Informação e Algoritmos.

Sumário

Parte I

A Linguagem Básica

Capítulo 1

Conjuntos

"-Comece pelo começo", disse o Rei de maneira severa,
"-E continue até chegar ao fim, então pare!"

Lewis Carroll, Alice no País das Maravilhas.

1.1 Sobre conjuntos e elementos

A ideia de conjunto é provavelmente o conceito mais fundamental compartilhado pelos mais diversos ramos da matemática. O primeiro grande estudioso que apresentou um relativo sucesso na missão de formalizar o conceito de conjunto, foi o matemático alemão George Cantor (1845-1918), em seu seminal trabalho [13]. Cantor apresentou as bases para o que hoje é chamada de teoria ingênua dos conjuntos. A seguir será apresentada uma tradução não literal da definição original de Cantor.

Definição 1.1 — Formalização por Cantor. Um **conjunto** A é uma **coleção** em uma totalidade $\mathbb{U}$ de **objetos** distintos e bem-definidos n que são parte da nossa percepção ou pensamento, tais objetos são chamados de **elementos** de A.

Agora note que a definição apresentada por Cantor distingue conjuntos e elementos como sendo objetos diferentes, e assim, a teoria dos conjuntos de cantor não tem um único objeto fundamental, mas dois, sendo eles, os conjuntos e os elementos. Além disso, a Definição 1.1 possui a exigência sobre dois aspectos da natureza dos elementos em um conjunto, a saber: (1) Os elementos devem ser distintos entre si[1] e (2) eles (os elementos) devem ser bem-definidos.

A definição de Cantor permite que sejam criados conjuntos com qualquer coisa que o indivíduo racional possa pensar ou perceber pelos seus sentidos. Agora,

[1]Em um conjunto não é permitido a repetição de elementos.

entretanto, deve-se questionar o que significa dizer que algo é bem-definido? Uma resposta satisfatória para essa perguntar é dizer que algo é bem-definido se esse algo pode ser descrito sem ambiguidades.

É claro que qualquer coisa pode ser descrita a partir de suas propriedades, isto é, por suas características (ou atributos). Sendo que essas propriedades sempre podem ser verificadas pelos sentidos no caso de objetos físicos, e sempre se pode pensar e argumentar sobre elas no caso de objetos abstratos. Assim pode-se modificar um pouco a definição de Cantor para a forma apresentada a seguir.

Definição 1.2 — Definição de Cantor Modificada. Um **conjunto** A é uma **coleção** numa totalidade $\mathbb{U}$ de certos **objetos** n distintos, que satisfazem certas propriedades, tais objetos são chamados de **elementos** de A.

Note que a Definição 1.2 permite concluir que um conjunto seja o agrupamento de entidades (os elementos) que satisfazem certas propriedades, ou ainda que, as propriedades definem os conjuntos. Prosseguindo nesse texto serão apresentadas as convenções da **teoria ingênua dos conjuntos** de forma usual, mas com um olhar de computação, isto é, apresentado os aspectos sintáticos e semânticos da teoria.

Tomando Notas 1.1 – Nomenclatura. É também muito comum em diversos textos, tais como [14] e [46], empregar termos como, **discurso**, **universo** ou **universo de estudo**, em vez de usar o termo **totalidade** encontrado nas Definições 1.1 e 1.2, ao se especificar um conjunto. Neste texto sempre que necessário será adotado o uso de **discurso**.

Prosseguindo com este documento, o primeiro passo será a apresentação da teoria dos conjuntos, é interessante notar que nas Definições 1.1 e 1.2, o objeto conjunto foi nomeado de forma arbitrária como A o discurso como $\mathbb{U}$ e os elementos como n, mas por qual razão foi usado isto? Essa estratégia é usado comumente na matemática, e a ideia por trás é atribuir a um objeto um "apelido", a seguir será formalizado esta ideia de forma mais precisa.

Definição 1.3 — Rótulo para conjuntos. Palavras (com ou sem indexação) formadas apenas por letras maiúsculas do alfabeto latino serão usadas como rótulos[a] que representam conjuntos.

[a] Aqui o leitor pode entender rótulo por um apelido dado ao conjunto.

A ideia de dar um rótulo ao conjunto se faz necessário visto o grande trabalho de escrita e leitura caso isso não fosse feito. Para ilustar considere a situação de que fosse necessário sempre se referir, por exemplo, ao **conjunto de todas as pessoas que moram em recife, mas que não são brasileiras com mais 40 anos e possuem dois filhos**. Ficar escrevendo sobre esse conjunto, seria altamente desgastante, assim não seria prático, dessa forma, é conveniente o uso de rótulos, isto é, a simbologia matemática, para torna texto e explicações mais dinâmicas. Os exemplos a seguir esboçam bem a ideia do uso de rótulos para designar conjuntos.

Exemplo 1.1 O conjunto de todas as pessoas que moram em recife, mas que não são brasileiras com mais 40 anos e possuem dois filhos, pode ser denotado simplesmente por PE_{40}, ou qualquer outra palavra nos padrões estabelecidos pela Definição 1.3.

Exemplo 1.2 O conjunto de todos os vizinhos da casa de número 4 pode ser representado por $VIZINHOS_4$, $VIZINHOS_{Casa_4}$, ou simplesmente V_4.

Exemplo 1.3 O Conjunto de todos os primos de Ana pode ser representado por A_{primos}, ANA_p ou ainda A_p.

Em diversas situações ao se trabalhar com conjuntos, como as apresentadas no capítulo inicial de [46], é necessário descrever um conjunto não por seu apelido (ou nome[2]), mas sim apresentando uma forma que descreva o conjunto de forma precisa e curta, seja listando (geralmente entre chaves e separados por vírgula) os elementos que juntos formam o referido conjunto, ou através da descrição da propriedade que descreve o conjunto, esta forma de representação costuma ser chamada representação compacta[3].

Exemplo 1.4 O conjunto dos números naturais[a] menores que 10 é escrito na notação compacta como $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, Já o conjunto dos naturais menores que 5 e maiores que 3 pode ser escrito usando a notação compacta como $\{x \mid 3 < x < 5\}$.

[a]Neste documento em virtude da formação acadêmica de seu autor, o número zero (0) é um número natural, esse ponto é discutível em outras obras.

Exemplo 1.5 A seguir são apresentados algumas instâncias de conjuntos não numéricos.

(a) $\{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$.

(b) {⚁, ⚂, ⚄}.

(c) {Flamengo, Fluminense, Palmeiras, São Paulo}.

(d) {5, a, ⚃, {$\spadesuit, \clubsuit$}}.

[2]No caso dos conjuntos numérico note que eles possuem nomes próprios, sendo: Naturais, Inteiros, Reais e etc. Sendo que o "apelido" para tais conjuntos são respectivamente os símbolos $\mathbb{N}, \mathbb{Z}$ e $\mathbb{R}$, tais símbolos funcionam como **palavras reservadas** dentro da teoria ingênua dos conjuntos, além dos conjuntos numéricos, o conjunto vazio também possui seu rótulo, sendo tal rótulo o símbolo $\emptyset$.

[3]Em outra obras como dito [71] na notação compacta é chamada de *Set builder*.

(e) $\{\text{Valdigleis}, \mathbb{C}, \{\bullet, \bullet\}, \{⚅\}\}$

Exemplo 1.6 O conjunto de todos inteiros múltiplos de 5 em notação compacta pode ser representado como $\{x \mid x = 5y, \text{ sendo } y \text{ um número inteiro}\}$.

Exemplo 1.7 O conjunto de números naturais maiores que 2 e menores que 13 pode ser representado como $\{x \mid 3 \leq x \leq 12\}$.

Tomando Notas 1.2 – Captura de variáveis. Muitas vezes[a] na notação compacta é necessário o uso de variáveis para descrever um conjunto, essas variáveis usadas tem a função de serem objetos "*dummy*" do conjunto[b]. Assim variáveis à esquerda do símbolo "|" podem ser trocadas por qualquer variável que não ocorre livre no lado direito de "|". Tome como exemplo o conjunto,

$$\{x \mid x = 5 + 2y\}$$

em tal conjunto, a variável x pode ser substituída pela variável z sem qualquer perda, ficando então com,

$$\{z \mid z = 5 + 2y\}$$

note porém contudo que se x fosse possível substituir x por y o conjunto então seria

$$\{y \mid y = 5 + 2y\}$$

o que seria absurdo por dois motivos, o primeiro é obviamente y não pode ser igual a $5 + 2y$, além disso, o y que era livre no conjunto tornou-se ligado ao conjunto, assim a referência ao y original do lado direito de | não pode ser mais recuperado.

[a] Em especial quando se descreve conjuntos infinitos.

[b] Aqui o termo *dummy* tem sentido similar ao encontrado em teoria das linguagens de programação, ou seja, entidades ou variáveis fictícias.

Para prosseguir, é interessante notar que nos itens "a", "b" e "c" apresentado no Exemplo 1.5, os elementos no conjunto têm a mesma natureza (ou tipo), por outro lado, os itens "d" e "e" apresentam a propriedade dos elementos no conjunto serem de tipos diferentes.

No primeiro caso, quando todos os elementos têm o mesmo tipo[4], é dito que

[4] Tipo aqui pode ser interpretado como um segmentar os elementos do conjunto em diferentes "espécies", não faz menção a área de matemática chamada teoria dos tipos [58].

o conjunto é **homogêneo**. Já no segundo caso, ou seja, quando os elementos no conjunto possuem tipos diferentes, é dito que o conjunto é **heterogêneo**. A seguir, mais exemplos são apresentados deste conceito.

Exemplo 1.8 A seguir alguns conjuntos homogêneos,

(a) $\{10, 20, 30, 40, 50\}$.

(b) $\{1, 2, 3, 4, 5\}$.

(c) $\{a, b, c, d, e\}$.

Exemplo 1.9 Os conjuntos a seguir são todos heterogêneos,

(a) $\{A, 10, \clubsuit, \bullet\}$.

(b) $\{\text{azul, vermelho, amarelo}, \sqrt{2\pi}\}$.

(c) $\{x, y, z, 1.27, \text{Linux, Darwin, DOS}\}$.

1.2 Pertinência, Inclusão e Igualdade

Em matemática ao se apresentar qualquer novo tipo de objeto é importante apresentar as interfaces[5] que são "*executadas*" sobre esse novo tipo de objeto, assim esta seção irá se dedicar a apresentar as três relações fundamentais sobre conjuntos, e algumas delas derivadas.

A primeira das interfaces para o conceito de conjunto que será aqui expressa é a pertinência, esta sendo representado pelo símbolo $\in$. A pertinência é a interface que funciona provocando a interação entre um elemento do discurso e um conjunto, a seguir é apresentado formalmente o conceito de pertinência.

Definição 1.4 — Pertinência. Seja A um conjunto definido sobre um discurso $\mathbb{U}$ por uma propriedade $\mathbf{P}$ e seja x um elemento do discurso. Se o elemento x possui (ou satisfaz) a propriedade $\mathbf{P}$, então é dito que x pertence a A, denotado por $x \in A$.

Assim note que a Definição 1.4 estabelece que, ao usar a pertinência é sempre escrito uma palavra da linguagem da teoria dos conjuntos tendo esta palavra a forma:

$$\underline{\qquad} \in \underline{\qquad}$$

o espaço em vermelho deve ser ocupado por elemento concreto do discurso ou por um símbolo de variável (um *dummy*) que represente os elementos no discurso. Já o espaço em azul deve ser ocupado por alguma representação de um conjunto, seja o rótulo ou a forma compacta do conjunto.

[5]Aqui interfaces diz respeito aos mecanismos que permitem a interação entre os objetos matemáticos.

A relação de pertinência é central para a definição de outras relações dentro da teoria dos conjuntos[6], o que permite enxergar a relação de pertinência como um dos pilares fundamentais da teoria. Um exemplo desta característica fundamental da pertinência no desenvolvimento de outras relações, é seu uso para definir a relação de inclusão apresentada à seguir.

Definição 1.5 — Relação de inclusão. [46] Dado dois conjuntos A e B quaisquer, é dito que A é subconjunto de (ou está incluso[a] em) B, denotado por $A \subseteq B$, quando todo $x \in A$ é tal que $x \in B$.

[a]Dualmente a relação de inclusão existe sua negação, isto é, a relação de não inclusão denotada por $\nsubseteq$.

Note que a Definição 1.5 estabelece a escrita,

$$\underline{\qquad} \subseteq \underline{\qquad}$$

onde os espaços em vermelho devem ser preenchidos com rótulos de conjuntos ou com a representação compacta, a seguir são apresentados usos da relação de inclusão.

Exemplo 1.10 Dado o conjunto $\mathbb{Z}$ tem-se que o conjunto,

$$N = \{x \mid x = 2k \text{ para algum } k \in \mathbb{Z}\}$$

é claramente um subconjunto de $\mathbb{Z}$, pois todo número par é também um número inteiro.

Exemplo 1.11 As seguintes relações de inclusão se verificam:

(a) $\{a, e, u\} \subseteq \{a, e, o, i, u\}$.

(b) $\{x \mid x \text{ é uma cidade do PE}\} \subseteq \{x \mid x \text{ é uma cidade do Brasil}\}$.

(c) $\{x \mid x = 2k \text{ para algum } k \in \mathbb{N}\} \subseteq \mathbb{N}$.

(d) $\{\text{Brasil}\} \subseteq \{x \mid x \text{ é um país do continente americano}\}$

É fácil notar que a inclusão estabelece que um conjunto A está incluso em outro conjunto B sempre que B contém todos os elementos de A, assim é claro que todo conjunto é subconjunto (ou seja está incluso) de si mesmo. Além disso, existem a possibilidade de A ser subconjunto de B, porém, pode acontecer de B conter elementos que não estejam em A, nesse cenário é dito que A é um subconjunto próprio de B, e isto é expresso pela palavra $A \subset B$.

Exemplo 1.12 As seguintes relações de inclusão se verificam:

[6]Dual a própria relação de pertinência existe a não pertinência $\notin$, definida formalmente como sendo a negação da relação de pertinência.

(a) $\{1, 2\} \subset \mathbb{R}$.

(b) $\{x \mid x \text{ é uma cidade do PE}\} \subset \{x \mid x \text{ é uma cidade do Brasil}\}$.

(c) $\mathbb{Z}^{+} \subset \mathbb{Z}$.

Uma propriedade interessante sobre a inclusão é que o conjunto vazio está incluso, ou seja, é subconjunto, de qualquer outro conjunto existente.

Teorema 1.1 Para todo conjunto A tem-se que $\emptyset \subseteq A$.

Demonstração. Suponha por absurdo que existe um conjunto A tal que $\emptyset \not\subseteq A$, assim por definição existe pelo menos um $x \in \emptyset$ tal que $x \notin A$, mas isto é um absurdo já que o vazio não possui elementos e, portanto, a afirmação que $\emptyset \not\subseteq A$ é falsa, logo, $\emptyset \subseteq A$ é uma asserção verdadeira para qualquer que seja o A. $\square$

Tomando Notas 1.3 – Pegando a dica sobre demonstrações. Neste documento ao final das demonstrações será sempre colocado o símbolo $\square$, tal símbolo é conhecido como túmulo de Halmos[a], este símbolo será usado para substituir a notação q.e.d. ("*quod erat demonstrandum*") usando por outras fontes bibliográficas para marcar o ponto de finalização de uma demonstração.

[a]Em inglês esse símbolo é conhecido como *tombstone*, e tal símbolo foi usado para marcar o final de uma demonstração inicialmente pelo matemático Paul Halmos (1916-2006).

Observação 1.1 — É sempre bom lembrar! É sempre bom lembrar que quando $A \subset B$, então é verdade que $A \subseteq B$. Mas o oposto não é verdade, basta lembrar que todo conjunto é subconjunto de se próprio, mas não pode ser subconjunto próprio.

Usando a ideia de subconjunto pode-se como apresentado na literatura em obras como [1, 30, 46] introduzir a ideia de igualdade entre conjuntos, esta noção é apresentada formalmente como se segue.

Definição 1.6 [1] Dois conjuntos A e B são iguais, denotado por $A = B$, se e somente se, $A \subseteq B$ e $B \subseteq A$.

Teorema 1.2 — Teorema da igualdade. Sejam A, B e C conjuntos quaisquer. Tem-se que:

1. $A = A$.
2. Se $A = B$, então $B = A$.
3. Se $A = B$ e $B = C$, então $A = C$.

Agora que foi apresentada a relação fundamental de pertinência, e as relação de inclusão e igualdade dela derivadas, pode-se agora prosseguir com este documento apresentando as operações básicas sobre conjuntos.

1.3 Operações sobre conjuntos

A organização com que está seção do documento irá apresentar as operações sobre conjuntos é a apresentada em [47].

Definição 1.7 — União de conjuntos. Sejam A e B dois conjuntos quaisquer, a união de A com B, denotada por $A \cup B$, corresponde ao seguinte conjunto.

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

Exemplo 1.13 Dados os dois conjuntos $A = \{x \in \mathbb{N} \mid x = 2i \text{ para algum } i \in \mathbb{N}\}$ e $B = \{x \in \mathbb{N} \mid x = 2j + 1 \text{ para algum } j \in \mathbb{N}\}$ tem-se que $A \cup B = \mathbb{N}$.

Exemplo 1.14 Seja $N = \{1, 2, 3, 6\}$ e $L = \{4, 6\}$ tem-se que $N \cup L = \{1, 4, 6, 3, 2\}$.

Como apontado em [46] alguns livros usam a notação $A + B$ para representar a união, é comum nesse caso não usar a nomenclatura união, em vez disso, é usado o termo soma de conjunto, entretanto, trata-se da mesma operação de união apresentada na definição anterior. Além disso, existe uma outra forma de união, chamada união de disjunta, em que é produzido um novo conjunto que contém copias dos conjuntos bases da união, e em que os elementos do conjunto produzido por essa união apresentam um "codigo[7]" que identifica de qual conjunto base o elemento veio, ainda não é possível formalizar este conceito de união disjunta neste capítulo, entretanto o mesmo será formalizado em capítulos futuros.

Definição 1.8 — Interseção de conjuntos. Sejam A e B dois conjuntos quaisquer, a interseção de A com B, denotada por $A \cap B$, corresponde ao seguinte conjunto.

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

A seguir são apresentados alguns exemplo da operação de interseção de conjuntos.

Exemplo 1.15 Seja $A = \{1, 2, 3\}, B = \{2, 3, 4, 5\}$ e $C = \{5\}$ tem-se que:

[7] Em alguns textos como em [14], é usado o termo chave em vez de código.

(a) $A \cap B = \{2, 3\}$.

(b) $A \cap C = \emptyset$.

(c) $B \cap C = \{5\}$.

Exemplo 1.16 Dado $A_1 = \{x \in \mathbb{N} \mid x \text{ é múltiplo de } 2\}$ e $A_2 = \{x \in \mathbb{N} \mid x \text{ é múltiplo de } 3\}$ tem-se que $A_1 \cap A_2 = \{x \in \mathbb{N} \mid x \text{ é múltiplo de } 6\}$.

Com respeito as propriedades equacionais das operações de união e interseção tem-se como exposto em [47] os seguintes resultados para qualquer três conjuntos A, B e C.

Propriedade	União	Interseção
(p_1) Idempotência	$A \cup A = A$	$A \cap A = A$
(p_2) Comutatividade	$A \cup B = B \cup A$	$A \cap B = B \cap A$
(p_3) Associatividade	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
(p_4) Distributividade	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(p_5) Neutralidade	$A \cup \emptyset = A$	$A \cap \mathbb{U} = A$
(p_6) Absorção	$A \cup \mathbb{U} = \mathbb{U}$	$A \cap \emptyset = \emptyset$

Tabela 1.1: Tabela das propriedades das operações de união e interseção.

Observação 1.2 — Referenciando propriedades Os verbetes p_1, p_2, p_3, p_4, p_5 e p_6 expressos na Tabela 1.1 são rótulos para referenciar as respectivas propriedades apresentadas no decorrer deste documento.

Além das propriedades apresentadas pela Tabela 1.1, a união e a interseção possuem propriedades ligadas a relação de inclusão.

Teorema 1.3 Para quaisquer conjuntos A e B tem-se que:

i. $A \subseteq (A \cup B)$.

ii. $(A \cap B) \subseteq A$

Demonstração. Direta das Definições 1.5, 1.7 e 1.8. □

A partir da definição de interseção é estabelecido um conceito de extrema valia para a teoria dos conjuntos e suas aplicações, tal conceito é o estado de disjunção entre dois conjuntos.

Definição 1.9 — Conjuntos disjuntos. Dois conjuntos A e B são ditos disjuntos sempre que $A \cap B = \emptyset$.

Exemplo 1.17 Seja $A = \{1, 2, 3\}, B = \{2, 3, 5\}$ e $C = \{5\}$ tem-se que A e C são disjuntos, por outro lado, A e B não são disjuntos entre si, além disso, B e C também não são disjuntos entre si.

Definição 1.10 — Complemento de conjuntos. Seja $A \subseteq \mathbb{U}$ para algum discurso $\mathbb{U}$, o complemento de A, denotado por $\overline{A}$, corresponde ao seguinte conjunto:

$$\overline{A} = \{x \in \mathbb{U} \mid x \notin A\}$$

Exemplo 1.18 Dado $P = \{x \in \mathbb{Z} \mid x = 2k \text{ para algum } k \in \mathbb{Z}\}$ tem-se então o seguinte complemento $\overline{P} = \{x \in \mathbb{Z} \mid x = 2k + 1 \text{ para algum } k \in \mathbb{Z}\}$.

Exemplo 1.19 Dado discurso $\mathbb{U}$ tem-se direto da definição que $\overline{\mathbb{U}} = \emptyset$, e obviamente, $\overline{\emptyset} = \mathbb{U}$.

Teorema 1.4 Dado um conjunto A tem-se que:

i. $A \cup \overline{A} = \mathbb{U}$.

ii. $A \cap \overline{A} = \emptyset$.

iii. $\overline{\overline{A}} = A$.

Demonstração. Direta das Definições 1.7, 1.8 e 1.10. □

Tomando Notas 1.4 – Um nome elegante A propriedade (iii) apresentada no Teorema 1.4 costuma ser chamada involução, como dito em [46].

Além das propriedades apresentadas no Teorema 1.4 o complemento também apresenta propriedades ligadas diretamente a união e a interseção, tais propriedades são uma versão conjuntistas das famosas leis De Morgan (ver [14, 48, 47]) muito conhecidas pelos estudiosos da área de lógica, a seguir são apresentadas as leis De Morgan para a linguagem teoria dos conjuntos.

(DM1) Primeira Lei De Morgan: $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$
(DM2) Segunda Lei De Morgan: $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

Seguindo com este texto, uma outra importante operação sobre conjuntos é a diferença entre dois conjuntos. A diferença entre conjunto apresenta duas formas, a primeira considerada por muito com a diferença natural [14], Já a segunda forma existente, é conhecida por diferença simétrica, esta segunda forma em um certo sentido, pode ser usada para medir a dissimetria entre conjuntos, ambas as operações são definidas formalmente a seguir.

Definição 1.11 — Diferença de conjuntos. Dado dois conjuntos A e B, a diferença de A e B, denotado por $A - B$, corresponde ao seguinte conjunto:

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

Exemplo 1.20 Dado os conjuntos $S = \{a, b, c, d\}$ e $T = \{f, b, g, d\}$ tem-se os seguintes conjuntos de diferença: $S - T = \{a, c\}$ e $T - S = \{f, g\}$.

Exemplo 1.21 Dado os conjuntos $\mathbb{Z}$ e $\mathbb{Z}_+^*$ tem-se que $\mathbb{Z} - \mathbb{Z}_+^* = \mathbb{Z}_-$.

Exemplo 1.22 Dado $A = \{1, 2, 3, 4\}$ tem-se que $A - \mathbb{N} = \emptyset$ e $A - \mathbb{Z}_- = A$.

Observação 1.3 — Cuidado com a Diferença ALiCIA já está brava só de pensar que você pode achar que a diferença de conjunto é comutativa, ela chama a sua atenção para o Exemplo 1.20, que mostra claramente que a operação de diferença de conjuntos não é comutativa. Então CUIDADO com o que você responde por ai!!!

Teorema 1.5 Para todo A e B tem-se que:

i. $A - B = A \cap \overline{B}$.

ii. Se $B \subset A$ e $A = \mathbb{U}$, então $A - B = \overline{B}$.

Demonstração. Dado os conjuntos A e B segue que:

i. Por definição para todo $x \in A - B$ tem-se que $x \in A$ e $x \notin B$, mas isto só é possível se, e somente se, $x \in A$ e $x \in \overline{B}$, e por sua vez, isto só é possível se, e somente se, $x \in A \cap \overline{B}$, portanto, tem-se que $A - B = A \cap \overline{B}$.

ii. Suponha que $B \subset A$, ou seja, todo $x \in B$ e tal que $x \in A$. Agora note que todo $x \in A - B$ é tal que $x \in A$ e $x \notin B$, e portanto, pela Definição 1.11 e pela hipótese de $B \subset A$ é claro que $A - B = \overline{B}$.

□

A seguir são apresentadas duas séries de igualdades notáveis relacionadas a diferença entre conjuntos.

Teorema 1.6 Sejam A e B conjuntos sobre um discurso $\mathbb{U}$, tem-se que:

a. $A - \emptyset = A$ e $\emptyset - A = \emptyset$.

b. $A - \mathbb{U} = \emptyset$ e $\mathbb{U} - A = \overline{A}$.

c. $A - A = \emptyset$.

d. $A - \overline{A} = A$.

e. $\overline{(A - B)} = \overline{A} \cup B$.

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

Demonstração. Para todas as equações a seguir suponha que A e B são conjuntos sobre um discurso $\mathbb{U}$ assim segue que:

a.

$$\begin{aligned} A - \emptyset &\overset{Teo.\ 1.5(i)}{=} A \cap \overline{\emptyset} \\ &= A \cap \mathbb{U} \\ &\overset{Tab.\ 1.1(p_5)}{=} A \end{aligned}$$

e também tem-se que,

$$\begin{aligned} \emptyset - A &\overset{Teo.\ 1.5(i)}{=} \emptyset \cap \overline{A} \\ &\overset{Tab.\ 1.1(p_6)}{=} \emptyset \end{aligned}$$

b. A prova tem um raciocínio similar a demonstração do item anterior, assim será deixado como exercício ao leitor.

c. Trivial pela própria Definição 1.11.

d.

$$\begin{aligned} A - \overline{A} &\overset{Teo.\ 1.5(i)}{=} A \cap \overline{\overline{A}} \\ &\overset{Teo.\ 1.4(iii)}{=} A \cap A \\ &\overset{Tab.\ 1.1(p_1)}{=} A \end{aligned}$$

e.

$$\begin{aligned} \overline{(A - B)} &\overset{Teo.\ 1.5(i)}{=} \overline{(A \cap \overline{B})} \\ &\overset{\textbf{(DM2)}}{=} \overline{A} \cup \overline{\overline{B}} \\ &\overset{Teo.\ 1.4(iii)}{=} \overline{A} \cup B \end{aligned}$$

f.

$$\begin{aligned} A - B &\overset{Teo.\ 1.5(i)}{=} A \cap \overline{B} \\ &\overset{Tab.\ 1.1(p_2)}{=} \overline{B} \cap A \\ &\overset{Teo.\ 1.4(iii)}{=} \overline{B} \cap \overline{\overline{A}} \\ &\overset{Teo.\ 1.5(i)}{=} \overline{B} - \overline{A} \end{aligned}$$

E assim a prova está concluída. □

Tomando Notas 1.5 – Referências em provas equacionais Na demonstração do Teorema 1.6 apresentada anteriormente, algumas vezes foi escrito o símbolo de $=$ com um texto acima, isso é uma técnica comum na escrita de demonstrações matemáticas, o entendimento que leitor precisa ter é que ao escrever $\overset{\kappa}{=}$ significa que a igualdade segue (ou é garantida) pela propriedade ou resultado κ. Durante este texto em algumas demonstrações uma escrita similar irá aparecer para outros símbolos além da igualdade, por exemplo, para o símbolo de implicação, que será introduzidos no decorrer deste documento.

Teorema 1.7 Sejam A, B e C subconjuntos de um discurso $\mathbb{U}$, tem-se que:

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

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

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

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

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

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

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

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

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

j. $(A - B) - B = A - B$.

Demonstração. Para todas as equações a seguir suponha que A, B e C são subconjuntos de um universo $\mathbb{U}$ assim segue que:

a.

$$
\begin{aligned}
(A-B)-C &\overset{Teo.\ 1.5(i)}{=} (A\cap\overline{B})\cap\overline{C}\\
&\overset{Tab.\ 1.1(p_3)}{=} A\cap(\overline{B}\cap\overline{C})\\
&\overset{\textbf{(DM1)}}{=} A\cap\overline{(B\cup C)}\\
&\overset{Teo.\ 1.5(i)}{=} A-(B\cup C)
\end{aligned}
$$

b.

$$
\begin{aligned}
A-(B-C) &\overset{Teo.\ 1.5(i)}{=} A\cap\overline{(B-C)}\\
&\overset{Teo.\ 1.6(e)}{=} A\cap(\overline{B}\cup C)\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap\overline{B})\cup(A\cap C)\\
&\overset{Teo.\ 1.5(i)}{=} (A-B)\cup(A\cap C)
\end{aligned}
$$

c.

$$
\begin{aligned}
A\cup(B-C) &\overset{Teo.\ 1.5(i)}{=} A\cup(B\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cup B)\cap(A\cup\overline{C})\\
&\overset{Tab.\ 1.1(p_2)}{=} (A\cup B)\cap(\overline{C}\cup A)\\
&\overset{Teo.\ 1.4(iii)}{=} (A\cup B)\cap(\overline{C}\cup\overline{\overline{A}})\\
&\overset{\textbf{(DM2)}}{=} (A\cup B)\cap\overline{(C\cap\overline{A})}\\
&\overset{Teo.\ 1.5(i)}{=} (A\cup B)-(C\cap\overline{A})\\
&\overset{Teo.\ 1.5(i)}{=} (A\cup B)-(C-A)
\end{aligned}
$$

d.

$$
\begin{aligned}
A\cap(B-C) &\overset{Teo.\ 1.5(i)}{=} A\cap(B\cap\overline{C})\\
&= \emptyset\cup(A\cap(B\cap\overline{C}))\\
&\overset{Tab.\ 1.1(p_2)}{=} \emptyset\cup((A\cap B)\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_6)}{=} (\emptyset\cap B)\cup((A\cap B)\cap\overline{C})\\
&\overset{Teo.\ 1.4(ii)}{=} ((A\cap\overline{A})\cap B)\cup((A\cap B)\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_2,p_3)}{=} ((A\cap B)\cap\overline{A})\cup((A\cap B)\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap B)\cap(\overline{A}\cup\overline{C})\\
&\overset{\textbf{(DM2)}}{=} (A\cap B)\cap\overline{(A\cap C)}\\
&\overset{Teo.\ 1.5(i)}{=} (A\cap B)-(A\cap C)
\end{aligned}
$$

e.

$$\begin{aligned}
A-(B\cup C) &\overset{Teo.\ 1.5(i)}{=} A\cap\overline{(B\cup C)}\\
&\overset{\textbf{(DM1)}}{=} A\cap(\overline{B}\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_1)}{=} (A\cap A)\cap(\overline{B}\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_3)}{=} ((A\cap A)\cap\overline{B})\cap\overline{C}\\
&\overset{Tab.\ 1.1(p_2,p_3)}{=} ((A\cap\overline{B})\cap A)\cap\overline{C}\\
&\overset{Tab.\ 1.1(p_3)}{=} (A\cap\overline{B})\cap(A\cap\overline{C})\\
&\overset{Teo.\ 1.5(i)}{=} (A-B)\cap(A-C)
\end{aligned}$$

f.

$$\begin{aligned}
A-(B\cap C) &\overset{Teo.\ 1.5(i)}{=} A\cap\overline{(B\cap C)}\\
&\overset{\textbf{(DM2)}}{=} A\cap(\overline{B}\cup\overline{B})\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap\overline{B})\cup(A\cap\overline{C})\\
&\overset{Teo.\ 1.5(i)}{=} (A-B)\cup(A-C)
\end{aligned}$$

g.

$$\begin{aligned}
(A\cup B)-C &\overset{Teo.\ 1.5(i)}{=} (A\cup B)\cap\overline{C}\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap\overline{C})\cup(B\cap\overline{C})\\
&\overset{Teo.\ 1.5(i)}{=} (A-C)\cup(B-C)
\end{aligned}$$

h.

$$\begin{aligned}
(A\cap B)-C &\overset{Teo.\ 1.5(i)}{=} (A\cap B)\cap\overline{C}\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap B)\cap(\overline{C}\cap\overline{C})\\
&\overset{Tab.\ 1.1(p_2,p_3)}{=} (A\cap\overline{C})\cap(B\cap\overline{C})\\
&\overset{Teo.\ 1.5(i)}{=} (A-C)\cap(B-C)
\end{aligned}$$

i.

$$\begin{aligned}
A-(A-B) &\overset{Teo.\ 1.5(i)}{=} A\cap\overline{(A\cap\overline{B})}\\
&\overset{\textbf{(DM2)}}{=} A\cap(\overline{A}\cup\overline{\overline{B}})\\
&\overset{Tab.\ 1.1(p_4)}{=} (A\cap\overline{A})\cup(A\cap\overline{\overline{B}})\\
&\overset{Teo.\ 1.4(ii)}{=} \emptyset\cup(A\cap\overline{\overline{B}})\\
&\overset{Tab.\ 1.1(p_5)}{=} A\cap\overline{\overline{B}}\\
&\overset{Teo.\ 1.4(iii)}{=} A\cap B
\end{aligned}$$

j.

$$
\begin{aligned}
(A - B) - B &\overset{Teo.\ 1.5(i)}{=} (A \cap \overline{B}) \cap \overline{B} \\
&\overset{Tab.\ 1.1(p_3)}{=} A \cap (\overline{B} \cap \overline{B}) \\
&\overset{Tab.\ 1.1(p_1)}{=} A \cap \overline{B} \\
&\overset{Teo.\ 1.5(i)}{=} A - B
\end{aligned}
$$

□

Para prosseguir com esta seção sobre as operações definidas sobre conjuntos será agora apresentada a última operação "clássica", sendo esta a diferença simétrica.

Definição 1.12 — Diferença simétrica. Dado dois conjuntos A e B, a diferença simétrica de A e B, denotado por $A \ominus B$, corresponde ao seguinte conjunto:

$$A \ominus B = \{x \mid x \in (A - B) \text{ ou } x \in (B - A)\}$$

Olhando atentamente a definição anterior é fácil notar que o conjunto da diferença simétrica é exatamente a união das possíveis diferenças entre os conjuntos, isto é, a diferença simétrica corresponde a seguinte igualdade: $A \ominus B = (A - B) \cup (B - A)$.

Exemplo 1.23 Seja $A = \{1, 2, 3\}$ e $B = \{3, 4, 5, 2\}$ tem-se que $A \ominus B = \{1, 4, 5\}$.

A seguir será apresentada uma série de importantes resultados com respeito a diferença simétrica.

Teorema 1.8 Sejam A e B subconjuntos quaisquer de um determinado universo $\mathbb{U}$, tem-se que $A \ominus B = (A \cup B) \cap \overline{(A \cap B)}$.

Demonstração. Dado A e B dois subconjuntos quaisquer de um determinado universo $\mathbb{U}$ segue que:

$$
\begin{aligned}
A \ominus B &= (A - B) \cup (B - A) \\
&\overset{Teo.\ 1.5(i)}{=} (A \cap \overline{B}) \cup (B \cap \overline{A}) \\
&\overset{Tab.\ 1.1(p_4)}{=} (A \cup (B \cap \overline{A})) \cap (\overline{B} \cup (B \cap \overline{A})) \\
&\overset{Tab.\ 1.1(p_4)}{=} ((A \cup B) \cap (A \cup \overline{A})) \cap ((\overline{B} \cup B) \cap (\overline{B} \cup \overline{A})) \\
&\overset{Teo.\ 1.4(i)}{=} ((A \cup B) \cap \mathbb{U}) \cap (\mathbb{U} \cap (\overline{B} \cup \overline{A})) \\
&\overset{Tab.\ 1.1(p_1,p_5)}{=} (A \cup B) \cap (\overline{B} \cup \overline{A}) \\
&\overset{\textbf{(DM2)}}{=} (A \cup B) \cap \overline{(B \cap A)}
\end{aligned}
$$

□

Corolário 1.1 Sejam A e B subconjuntos quaisquer de um determinado discurso $\mathbb{U}$, tem-se que $A \ominus B = (A \cup B) - (A \cap B)$.

Demonstração. Pelo Teorema 1.8 tem-se que $A \ominus B = (A \cup B) \cap \overline{(A \cap B)}$, mas pelo Teorema 1.5 (i) segue que $(A \cup B) \cap \overline{(A \cap B)} = (A \cup B) - (A \cap B)$, e portanto, $A \ominus B = (A \cup B) - (A \cap B)$. □

O próximo resultado mostra que a operação de diferença simétrica entre conjunto possui elemento neutro, isto é, existe um conjunto que quando operado com qualquer outro conjunto A, o resultado é o próprio conjunto A.

Teorema 1.9 Para todo A tem-se que $A \ominus \emptyset = A$.

Demonstração. Dado um conjunto A qualquer pelo Corolário 1.1 tem-se que $A \ominus \emptyset = (A \cup \emptyset) - (A \cap \emptyset)$, mas pelas propriedades apresentadas na Tabela 1.1 tem-se: $A \cup \emptyset = A$ e $A \cap \emptyset = \emptyset$. Logo $A \ominus \emptyset = A - \emptyset$, por fim, pelo Teorema 1.6 (a) tem-se que $A - \emptyset = A$, consequentemente, $A \ominus \emptyset = A$. □

Seguindo com as propriedades que a operação de diferença simétrica possui, o próximo resultado mostra a existência de um elemento que neste texto será chamado de **alternador**, isto é, existe um conjunto que quando operado com qualquer outro conjunto A, o resultado é o complemento deste conjunto A.

Teorema 1.10 Para todo A tem-se que $A \ominus \mathbb{U} = \overline{A}$.

Demonstração. Similar a demonstração do Teorema 1.9, ficando assim como exercício ao leitor. □

O teorema a seguir mostra que a diferença simétrica entre um conjunto A e seu complementar $\overline{A}$ é exatamente igual a totalidade do universo do discurso em que estes conjuntos estão inseridos.

Teorema 1.11 Para todo A tem-se que $A \ominus \overline{A} = \mathbb{U}$.

Demonstração. Dado um conjunto A qualquer e seu complementar $\overline{A}$ tem-se pelo Corolário 1.1 que $A \ominus \emptyset = (A \cup \overline{A}) - (A \cap \overline{A})$, mas pelo Teorema 1.4 tem-se que $A \cup \overline{A} = \mathbb{U}$ e $A \cap \overline{A} = \emptyset$, consequentemente, $A \ominus \emptyset = \mathbb{U} - \emptyset$, mas pelo Teorema 1.6 tem-se que $\mathbb{U} - \emptyset = \mathbb{U}$, e portanto, $A \ominus \overline{A} = \mathbb{U}$. □

Continuando a estudar a diferença simétrica o próximo teorema mostra que a diferença simétrica entre um conjunto A e ele mesmo é exatamente igual ao conjunto vazio.

Teorema 1.12 Para todo A tem-se que $A \ominus A = \emptyset$.

Demonstração. Dado um conjunto A qualquer tem-se pelo Corolário 1.1 que vale a seguinte igualdade, $A \ominus A = (A \cup A) - (A \cap A)$. Mas pelas propriedades apresentadas na Tabela 1.1 tem-se que $(A \cup A) = (A \cap A) = A$, logo $A \ominus A = A - A$, mas pelo Teorema 1.6 tem-se que $A - A = \emptyset$, portanto, $A \ominus A = \emptyset$. □

Anteriormente foi mostrado que a diferença entre conjuntos não era comutativa (Exemplo 1.20), o próximo resultado contrasta esse fato com respeito a diferença simétrica.

Teorema 1.13 Para todo A e B tem-se que $A \ominus B = B \ominus A$.

Demonstração. Dado dois conjuntos A e B tem-se pelo Corolário 1.1 que vale a seguinte igualdade, $A \ominus B = (A \cup B) - (A \cap B)$, mas pela propriedade de comutatividade de $\cup$ e de $\cap$ (ver Tabela 1.1) tem-se que $A \cup B = B \cup A$ e $A \cap B = B \cap A$, logo tem-se que $A \ominus B = (B \cup A) - (B \cap A)$, mas pelo Corolário 1.1 tem-se que $(B \cup A) - (B \cap A) = B \ominus A$, e portanto, $A \ominus B = B \ominus A$. □

Teorema 1.14 Para todo A, B e C tem-se que $(A \ominus B) \ominus C = A \ominus (B \ominus C)$.

Demonstração. A prova deste teorema sai direto da definição de diferença simétrica e assim ficará como exercício ao leitor. □

Teorema 1.15 Para todo A e B tem-se que $\overline{(A \ominus B)} = (A \cap B) \cup (\overline{A} \cap \overline{B})$.

Demonstração. Para todo A e B segue que:

$$
\begin{aligned}
\overline{(A \ominus B)} &\overset{Teo.\ 1.8}{=} \overline{((A \cup B) \cap \overline{(A \cap B)})} \\
&\overset{\textbf{(DM2)}}{=} \overline{(A \cup B)} \cup \overline{\overline{(A \cap B)}} \\
&\overset{\textbf{(DM1)}}{=} (\overline{A} \cap \overline{B}) \cup \overline{\overline{(A \cap B)}} \\
&\overset{\textbf{(DM2)}}{=} (\overline{A} \cap \overline{B}) \cup \overline{(\overline{A} \cup \overline{B})} \\
&\overset{\textbf{(DM1)}}{=} (\overline{A} \cap \overline{B}) \cup (\overline{\overline{A}} \cap \overline{\overline{B}}) \\
&\overset{Tab.\ 1.1(p_2)}{=} (\overline{\overline{A}} \cap \overline{\overline{B}}) \cup (\overline{A} \cap \overline{B}) \\
&\overset{Teo.\ 1.4(iii)}{=} (A \cap B) \cup (\overline{A} \cap \overline{B})
\end{aligned}
$$

□

1.4 Partes e Partições

Para concluir esta breve introdução à teoria ingênua dos conjuntos, nesta seção serão trabalhados dois importantes conceitos, as ideias de partes e partições. Ambos conceitos são conjuntos em que os elementos destes são também conjuntos.

O conceito de partes é de suma importância em diversos ramos da matemática, tais como Topologia[45] e linguagens formais[43, 8]. Já as partições são de interesse tanto teoricos[14, 30] quanto práticos, em especial, na área de agrupamento de dados[15, 27].

Definição 1.13 — Conjunto das partes. Seja A um conjunto. O conjunto das partes[a] de A, é denotada por $\wp(A)$, e corresponde ao seguinte conjunto:

$$\wp(A) = \{x \mid x \subseteq A\}$$

[a] Em alguns livros é usado o termo conjunto potência em vez do termo conjunto das partes, nesse caso é usado a notação 2^A para denotar o conjunto partes, por exemplo ver [47].

Uma propriedade interessante do conjuntos das partes como dito em [46], é que se A for da forma $A = \{x_1, \cdots, x_n\}$ para algum $n \in \mathbb{N}$, então pode-se mostrar que $\wp(A)$ terá exatamente 2^n elementos.

Exemplo 1.24 Seja $A = \{a, b, c\}$ tem-se que o conjunto das parte de A corresponde ao conjunto $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{c, b\}, \{a, b, c\}\}$.

Exemplo 1.25 Dado o conjunto $X = \{1\}$ tem-se que $\wp(X) = \{\emptyset, \{1\}\}$.

Exemplo 1.26 Seja $A = \emptyset$ tem-se que $\wp(A) = \{\emptyset\}$.

Além do conjunto das partes, os conjuntos gerados pela ideia da partição de um conjunto é de extrama importância em diversos segmentos do conhecimento, como comentado anteriormente, a seguir é apresentado formalmente a ideia de partições.

Definição 1.14 — Partição. Seja A um conjunto não vazio, uma partição é um conjunto não vazio de subconjuntos disjuntos de A, ou seja, uma partição é da forma $\{x_i \mid x_i \subseteq A\}$ tal que as seguintes condições são satisfeitas:

(1) Para todo $y \in A$ tem-se que existe um único i tal que $y \in x_i$ para algum $x_i \subseteq A$.

(2) Para todo i e todo j sempre que $i \neq j$, então $x_i \cap x_j = \emptyset$.

É fácil notar pela Definição 1.14 que partições são conjuntos, além disso, como dito em [47] os elementos em uma partição são chamados de **células**, isto é, dado um conjunto A os subconjuntos na partição de A são vistos como as células que formam o próprio conjunto A. O resultado a seguir garante que sempre é possível obter pelo menos uma partição de um conjunto.

Teorema 1.16 Se A é um conjunto não vazio, então existe pelo menos uma partição de A.

Demonstração. Suponha que o conjunto A seja não vazio, assim defina o conjunto $PT_A = \{\{x\} \mid x \in A\}$, agora claramente tem-se que PT_A é uma família e satisfaz todas as condições da Definição 1.14 e, portanto, PT_A é uma partição do conjunto A. $\square$

Tomando Notas 1.6 – Uma partição especial Apesar de não ter um nome específico a partição descrita no Teorema 1.16, é muito importante como ponto de partida para a construção de partições mais complexas, por esse fato neste documento será chamada de **partição trivial**.

1.5 Questionário

Questão 1.1 Para cada um dos conjuntos a seguir, determine uma propriedade que define o conjunto e escreva os conjuntos na notação compacta.

(a). $\{0, 2, 4, 6, 8, 1, 3, 5, 7, 9\}$.

(b). $\{-2, -4, -6, -8, 0, 6, 4, 8, 2\}$.

(c). $\{3, 5, 7, 9, 11, 13, 15, 17, \cdots\}$.

(d). $\{a, c, s\}$

(e). $\{2, 3, 5, 7, 11, 13, 17, 19, \cdots\}$.

(f). $\{1, 4, 9, 16, 25, 36, 64, 81, 100\}$.

(g). $\{3, 6, 9, 12, 15, 18, 21, \cdots\}$.

(h). $\left\{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}, \frac{5}{10}, \cdots\right\}$

Questão 1.2 Escreva os seguintes conjuntos em notação compacta.

(a). Conjunto de todos os países da América do sul.

(b). Conjunto de planetas do sistema solar.

(c). Conjunto dos números reais maiores que 1 e menores que 2.

(d). Conjunto de estados brasileiros cujo nome começa com a letra “R”.

(e). Conjunto dos times nordestinos que já foram campões da primeira divisão do campeonato brasileiro de futebol.

Questão 1.3 Escreva as sentenças a seguir de forma apropriada usando a linguagem da teoria dos conjuntos.

(a). x não pertence ao conjunto A.

(b). -2 não é um número natural.

(c). O símbolo π representa um número real.

(d). O conjunto das vogais não é subconjunto do conjunto das consoantes.

(e). y é um número inteiro, porém não é um número maior que 10.

(f). D é o conjunto de todos os múltiplos de -3 que são maiores que 1.

Questão 1.4 Considere o conjunto de letras $K = \{b, t, s\}$ responda falso ou verdadeiro e justifique sua resposta:

(a). $s \in K$?

(b). $t \subset K$?

(c). $K \not\subseteq K$?

(d). $\{b\} \in K$?

(e). $K - \{a\} = K$?

Questão 1.5 Identifique se o conjunto é Homogêneo ou Heterogêneo.

(a). $\{x, y, z, w\}$

(b). $\{2, 4, 6, 8, 10\}$

(c). $\{3, 5, 7, 9, 11\}$

(d). $\{1, a, 3.14, \text{“hello”}\}$

(e). $\{red, green, blue, yellow\}$

(f). $\{15, 20, 25, 30\}$

(g). $\{apple, banana, orange, pear\}$

(h). $\{x, y, 3, 5, 7\}$

(i). $\{100, 200, 300, 400\}$

(j). $\{0.5, 1.25, 3, 5, 7\}$

(k). $\{black, white, gray, brown\}$

(l). $\{cat, dog, fish, bird\}$

(m). $\{a, e, i, o, u\}$

(n). $\{January, February, March, April\}$

(o). $\{1, 2, 4, 8, 16\}$

(p). $\{x, y, z, 10, 20\}$

(q). $\{Monday, Tuesday, Wednesday, Thursday, Friday\}$

Questão 1.6 Considere cada conjunto a seguir e escreva todos os seus subconjuntos.

(a). $B = \{1, 2, 3\}$.

(b). $F = \{a, b, c, d\}$.

(c). $N = \{\emptyset\}$.

(d). $R = \{\emptyset, \{\emptyset\}\}$.

(e). $P = \{\{a, b\}, \{c, d\}, \{a, f\}, \{a, b, c\}, \emptyset\}$.

Questão 1.7 Considerando o universo dos números naturais, dado os subconjuntos: $A = \{1, 2, 3, 4, 5\}$, $B = \{x \in \mathbb{N} \mid x^2 = 9\}$, $C = \{x \in \mathbb{N} \mid x^2 - 4x + 6 = 0\}$ e $D = \{x \in \mathbb{N} \mid x = 2k$ para algum $k \in \mathbb{N}\}$, complemente as palavras com os símbolos $\subseteq$ e $\not\subseteq$.

(a). A ____ B.

(b). C ____ B.

(c). D ____ C.

(d). B ____ A.

(e). A ____ D.

(f). C ____ A.

(g). D ____ B.

(h). B ____ $\mathbb{N}$.

(i). $\mathbb{N}$ ____ D.

(j). A ____ $\mathbb{N}$.

(k). A ____ $\mathbb{Z}_-$.

(l). $\mathbb{N}$ ____ D.

(m). $\mathbb{N}$ ____ C.

(n). C ____ $\mathbb{N}$.

(o). $\{6\}$ ____ C.

Questão 1.8 Complete as palavras da teoria dos conjuntos com $\in, \subseteq$ e $\not\subseteq$.

(a). $\{2, \emptyset\}$____$\{1, 2, 3\}$.

(b). $\{2\}$____$\{1, 2, 3\}$.

(c). $\{1\}$____$\{\{1\}, \{2\}, \{3\}\}$.

(d). $\emptyset$____$\{1\}$.

(e). $\emptyset$____$\{\emptyset\}$.

(f). $\{3\}$____$\emptyset$.

(g). $\mathbb{N}$____$\{2,3,6\}$.

(h). $\{\{\emptyset\},\emptyset\}$____$\{\{\{\emptyset\},\emptyset\},\emptyset\}$.

(i). $\{a\}$____$\{\{a\},\{b\}\}$____$\{a,b,c\}$.

(j). $\{\{0\}\}$____$\mathbb{Z}_+^*$.

(k). $\left\{\frac{1}{0},-4\right\}$____$\mathbb{Q}$.

(l). $\{0,1\}$____$\{0,1,2,5\}$____$\mathbb{N}$.

(m). $\mathbb{N}$____$\wp(\mathbb{N})$

(n). $\emptyset$____$\emptyset$.

(o). $\{1,2,4\}$____$\{2,4,6\}$____$\{y \mid y = 2x \text{ para algum } x \in \mathbb{N}\}$.

(p). $\{1\}$____$\mathbb{R}$.

(q). $\left\{\frac{3}{4}\right\}$____$\mathbb{N}$.

Questão 1.9 Justifique as seguintes afirmações.

(a). $\left\{\frac{2}{x} \mid x-1>0 \text{ com } x \in \mathbb{N}\right\}$ não é subconjunto de $\mathbb{N}$.

(b). $\{2,3,4,6,8\}$ não é subconjunto de $\{x \in \mathbb{N} \mid x = 2k \text{ para algum } k \in \mathbb{N}\}$.

(c). $\{1,2,3\}$ é um subconjunto próprio do conjunto $\{1,2,3,4,5,6,7,8,9,0\}$.

(d). $\{0,5\}$ é subconjunto de $\mathbb{Z}$ mas não é subconjunto de $\mathbb{Z}^*$.

(e). $\{x \mid x+x=x\}$ é subconjunto próprio de $\mathbb{N}$.

(f). Existem exatamente 15 subconjuntos próprios do conjunto $\{2,3,5,7\}$.

(g). Não existem subconjuntos próprios do conjunto $\emptyset$.

(h). Sempre que $A \subset B$ e $A_0 \subset A$, tem-se que A_0 é também um subconjunto próprio de B.

(i). O conjunto $\{2\}$ tem um único subconjunto próprio.

(j). O conjunto $\{x \in \mathbb{N} \mid 0 < x < 3\}$ tem exatamente 3 subconjuntos próprios.

Questão 1.10 Considerando o universo $\mathbb{U} = \{1,2,3,4,5,6,7,8,9,0\}$ e seus subconjuntos $A = \{2,4,6,8\}$, $B = \{1,3,5,7,9\}$, $C = \{1,2,3,4,0\}$ e $D = \{0,1\}$ exiba os conjuntos a seguir.

(a). $A \cup B$.

(b). $C \cup D$.

(c). $D \cap A$.

(d). $B \cap C$.

(e). $A \cap (B \cup D)$.

(f). $D \cap (A \cap C)$.

(g). $(A \cap B) \cup (D \cap C)$.

(h). $(\mathbb{U} \cap A) \cup D$.

(i). $(D \cup A) \cap C$

(j). $D \cap (B \cup A)$

(k). $A \cup \overline{B}$.

(l). $\overline{(C \cap B)} \cup D$.

(m). $\overline{D \cap A}$.

(n). $B \cap \overline{C}$.

(o). $A \cap \overline{(\overline{B} \cup D)}$.

(p). $D \cap (A \cap C)$.

(q). $\overline{(A \cap B)} \cup (\overline{D} \cap C)$.

(r). $\overline{(\mathbb{U} \cap \overline{A})} \cup D$.

(s). $(D \cup A) \cap \overline{C}$

(t). $\overline{D \cap (B \cup A)}$

(u). $\overline{D - A}$.

(v). $(A - B) \cap \overline{C}$.

(w). $A \cap \overline{(\overline{B} - D)}$.

(x). $D \cap (A - C)$.

(y). $\overline{C} - D$.

(z). $D - A$.

Questão 1.11 Considerando o universo $\mathbb{U} = \{a, b, c, d, e, f, g, h, i, j\}$ e seus subconjuntos $A = \{b, d, f, h\}$, $B = \{a, c, e, g, i\}$, $C = \{a, b, c, d, j\}$ e $D = \{a, j\}$ exiba os seguintes conjuntos.

(a). $\overline{B} - C$.

(b). $A - (B \cup D)$.

(c). $(A - (A \cap B)) - ((\overline{D} \cap C) - A)$

(d). $\overline{(\mathbb{U} - \overline{C})} - D$

(e). $A \ominus (B \cup D)$.

(f). $(A \ominus (A \cap B)) \ominus ((\overline{D} \cap C) \ominus A)$

(g). $\overline{(\mathbb{U} \ominus \overline{C})} \ominus D$

(h). $\overline{D \ominus A}$.

(i). $(A \ominus B) \cap \overline{C}$.

(j). $\overline{C} \ominus D$.

(k). $D \ominus A$.

(l). $\overline{B} \ominus C$.

(m). $A \cap \overline{(\overline{B} \ominus D)}$.

(n). $D \cap (A \ominus C)$.

Questão 1.12 Uma aluna do curso de Ciência da Computação realizou uma pesquisa sobre três ritmos (A, B e C) presentes no aplicativo de música *Spotify* com seus colegas de classe para seu trabalho na disciplina de estatística, e levantou os dados expostos na Tabela 1.2.

Total de entrevistados	Ouvem A	Ouvem B	Ouvem C	Ouvem A e B	Ouvem A e C	Ouvem B e C	Ouvem A, B e C	Não ouvem nenhum
23	8	4	6	2	3	1	1	10

Tabela 1.2: Tabela com dados fictício da pesquisa sobre ritmos no *Spotify*.

(a). Qual é o número de entrevistados que escutam apenas o ritmo A?

(b). Qual é o número de entrevistados que escutam o ritmo A e não escutam o ritmo B?

(c). Quantos entrevistados não escutam o ritmo C?

(d). Qual é o número de entrevistados que escutam algum dos ritmos?

(e). Quantos entrevistados escutam o ritmo B ou C, mas não escutam o ritmo A?

Questão 1.13 Dado os conjuntos $A = \{1, 2, 3\}, B = \{3, 4, 5\}$ e $C = \{1, 5, 6\}$ construa um conjunto X com exatamente 4 elementos tal que $A \cap X = \{3\}$, $B \cap X = \{3, 5\}$ e $C \cap X = \{5, 6\}$.

Questão 1.14 Considere o banco de dados representado na Tabela 1.3. para esboçar o conjunto gerado por cada *Query* detalhada abaixo, relacionando as mesmas com as operações sobre conjuntos..

(a). O conjuntos dos id's onde o sexo é igual a F e o salário não é inferior a $2.000,00$.

(b). O conjunto dos salários em que a idade não é superior a 35 ou o sexo é igual a M.

(c). O conjunto de todos os nome em que a idade não é maior que 30 ou id é menor que 65.

id	Nome	Salário	Idade	Sexo
23	Júlio	2.300,00	34	M
102	Patrícia	4.650,00	23	F
33	Daniel	1.375,00	20	M
43	Renata	6.400,00	24	F
53	Rafaela	1.800,00	19	F
57	Tadeu	14.450,00	54	M

Tabela 1.3: Uma base de dados representada como uma tabela.

Questão 1.15 Exiba os seguintes conjuntos.

(a). $\wp(\{1,2,3\})$.

(b). $\wp(\wp(\{0,1\}))$.

(c). $\wp(\{\mathbb{N}\})$.

(d). $\wp(\{1,\{2\},\{1,\{2\}\}\})$.

(e). $\wp(\{1,\{1\},\{2\},\{3,4\}\})$.

(f). $\wp(\wp(\{1,2\})) - \wp(\{0,1\})$.

(g). $\wp(\{a,b,c,g\} \ominus \{g,e,f,d\})$.

(h). $\wp(\wp(\wp(\{0,1\})) \cup \wp(\{1,2,3\}))$.

(i). $\wp(\wp(\emptyset) - \emptyset)$.

(j). $\wp(\{2,3,4\} \cap (\{-1,3\} \cup \{-5\}))$.

Questão 1.16 Considere o universo $\mathbb{U} = \{a,b,c,d,e,f,g\}$ e seus subconjuntos $A = \{d,e,g\}, B = \{a,c\}, C = \{b,e,g\}$ calcule e exiba os seguintes conjuntos.

(a). $\wp(C)$.

(b). $\wp(A) - \wp(\overline{B})$.

(c). $\wp((A \cup B) \ominus C)$.

(d). $\wp((\overline{A} \cup B)) \ominus \wp(C)$.

(e). $\wp(\overline{(C \cap B)} - (\overline{A} \cap C))$

(f). $\wp(C) - (\wp(A) \ominus \wp(B))$.

(g). $\wp(\overline{A}) \ominus ((\wp(C) \cap \wp(B)) - \wp(A))$.

(h). $\wp(\wp(A)) - \wp(\wp(B))$.

(i). $\wp(\wp(\overline{C})) \ominus \wp(\wp(B))$.

(j). $\wp(\mathbb{U})$.

Questão 1.17 Dado o conjunto $A = \{a, b, c, d, e, f, g\}$ diga se as famílias de conjuntos a seguir são ou não partições de A, justifique todas as suas resposta.

(a). $P_1 = \{\{a, c, e\}, \{b\}, \{d, g\}\}$.

(b). $P_2 = \{\{a, g, e\}, \{c, d\}, \{b, e, f\}\}$.

(c). $P_3 = \{\{a, b, e, g\}, \{c\}, \{d, f\}\}$.

(d). $P_4 = \{\{a, b, c, d, e, f, g\}\}$.

(e). $P_5 = \{\{a, b, d, e, g\}, \{f, c\}\}$.

(f). $P_6 = \{\{a, b, c, d, e\}, \{e, f, g\}\}$.

(g). $P_7 = \{\{b, c, d, e, f, g\}, \{a\}, \{b, a, c\}\}$.

(h). $P_8 = \{\{a, b, c, d, e, f, g\}, \{e, d\}\}$.

(i). $P_9 = \{\{a\}, \{b\}, \{c\}, \{d, e\}, \{f\}, \{g\}\}$.

(j). $P_{10} = \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \{g\}\}$.

Questão 1.18 Considere o universo $\mathbb{U} = \{a, b, c, d, e, f, g\}$ e seus subconjuntos $A = \{d, e, g\}, B = \{a, c\}, C = \{b, e, g\}$ exiba duas partições diferentes da partição trivial para cada um dos conjuntos a seguir.

(a). $C - \overline{A}$.

(b). $A - \overline{B}$.

(c). $(A \cup B) \ominus C$.

(d). $(\overline{A} \cup B)) \ominus C$.

(e). $\overline{(C \cap B)} - (\overline{A} \cap C)$

(f). $C - (A \ominus B)$.

(g). $\overline{A} \ominus ((C \cap B) - A)$.

(h). $A - B$.

(i). $\overline{C} \ominus B$.

(j). $\wp(\mathbb{U})$.

Capítulo 2

Demonstrações

"Mais um colchão, mais uma demonstração".

Paul Erdös

"Um matemático é uma máquina que transforma café em teoremas".

Paul Erdös

2.1 Introdução

No Capítulo 1 deste documento, o leit]or encontrou diversas demonstrações dentro da teoria (Cantoriana) dos conjuntos. Para um leitor iniciantie, talvez tenha sido um tanto quanto complicado entender a metodologia usada para construir tais demonstrações. E desde que, as demonstrações são figuras de interesse central no cotidiano dos matemáticos, cientistas da computação e engenheiros de software, em especial aqueles que trabalham com métodos formais, este texto irá fazer uma breve pausa no estudo da teoria dos conjuntos, para apresentar um pouco de teoria da prova ao leitor.

Este capítulo começa então com o seguinte questionamento: "Do ponto de vista da ciência da computação, qual a importância das demonstrações?" Bem, a resposta a essa pergunta pode ser dada de dois pontos de vista, um teórico (purista) e um prático (aplicado ou de engenharia).

Na perspectiva de um cientista da computação puro, as demonstrações de teoremas, proposições, lema, corolários e propriedades são a principal ferramenta para investigar os limites dos diferentes modelos de computação propostos [34, 43], assim sendo é de suma importância que o estudante de graduação em ciência da computação receba em sua formação pelo menos o básico para dominar a "arte" de provar teoremas, sendo assim preparado para o estudo e a pesquisa pura em computação e(ou) matemática.

Já na visão prática, só existe uma forma segura de garantir que um *software* está livre de erros, essa “tecnologia” é exatamente a demonstração das propriedades do *software*. É claro que, mostrar que um *software* não possui erros vai exigir que o *software* seja visto através de um certo nível de formalismo e rigor matemático, mas após essa modelagem através de demonstrações pode-se garantir que um *software* não apresentará erros (quando bem especificado), e assim se algo errado ocorrer foi por fatores externos, tais como defeito no *hardware* por exemplo, e não por falha ou erros com a implementação. Este conceito é o cerne de uma área da engenharia de *software* [64], chamada métodos (ou especificações) formais, sendo essa área o ponto crucial no desenvolvimento de *softwares* para sistemas críticos [68]. Isto já mostra a grande importância de programadores e engenheiros de *software* terem em sua formação as bases para o domínio das técnicas de demonstração.

Nas próxima seções deste documento serão descritas as principais técnicas de demonstração de interesse de matemáticos, cientistas da computação e engenheiros formais de *software*.

Observação 2.1 — Uma dica valiosa! Para o leitor que nunca antes teve contato com a lógica matemática, recomenda-se que antes de estudar este capítulo, o leitor deve fazer pelo menos uma leitura superficial em obras como [21, 33, 48].

Para poder falar sobre métodos de demonstração e poder então descrever como os matemáticos, lógicos e cientistas da computação justificam propriedades usando apenas a argumentação matemática, será necessário fixar algumas nomenclaturas e falar sobre alguns conceitos importantes.

Definição 2.1 — Asserção. Uma **asserção** é qualquer frase declarativa que possa ser expressa na linguagem da lógica simbólica.

Os métodos (ou estratégias) de demonstrações apresentadas neste documento seguem as ideias e a ordem de apresentação similar ao que foi exposto em [72]. Em [72] antes de apresentar as provas formais, erá necessário a construção de um rascunho de prova, este rascunho possui similaridades com as demonstrações em provadores de teoremas tais como Coq [10, 62] e Lean [56], isto é, existe uma separação clara entre dados (hipótese) e os objetivos (em inglês *Goal*) que se quer demonstrar.

Neste documento por outro lado, não será utilizado a ideia de um rascunho de prova, em vez disso, será usado aqui a noção de **diagrama de blocos** [12]. Aqui tais diagramas serão encarados como as demonstrações em si, assim diferente de [72] não haverá a necessidade de escrever um texto formal após o diagrama da prova ser completado.

Sobre o diagrama de blocos é conveniente explicar sua estrutura, ele consiste de uma série de linhas numeradas de 1 até m, em cada linha está uma informação, sendo esta uma hipótese assumida como verdadeira ou deduzida a partir das informações anteriores a ela ou ainda um resultado (ou definição) válido(a) conhecido(a). Um diagrama de bloco representa uma prova, porém, uma prova pode conter n subprovas. Cada **prova** é delimitada no diagrama por um **bloco**, assim se existe uma subprova p' em uma prova p, significa que o diagrama de bloco de p' é interno ao diagrama de bloco de p. Na linha abaixo de todo bloco sempre estará a conclusão que se queria demonstrar, isto é, abaixo de cada bloco está a asserção que tal bloco demonstra.

Cada linha no diagrama começa com algum termo reservado (em um sentido similar ao de palavra reservada de linguagem de programação [3, 16]) escrito em negrito[1], esses termos reservados tem três naturezas distintas: inicialização de bloco, ligação e conclusão de blocos. Tais palavras podem variar a depender do material sobre demonstrações que o leitor possa encontrar na literatura neste documento serão usando os seguintes conjuntos de palavras:

- Termos de inicialização de bloco: **Suponha**, **Deixe ser**, **Assuma** e **Considere**;
- Termos de ligação: **mas**, **tem-se que**, **então**, **assim**, **logo**, **além disso**, **desde que** e **dessa forma**;
- Termos de conclusão de bloco: **Portanto**, **Dessa forma**, **Consequentemente**, **Por contrapositiva** e **Logo por contrapositiva**.

Exemplo 2.1 Demonstre a asserção: Dado $A = \{x \in \mathbb{Z} \mid x = 2i, i \in \mathbb{Z}\}$ e $B = \{x \in \mathbb{Z} \mid x = 2j - 2, j \in \mathbb{Z}\}$ tem-se que $A = B$.

1. **Assuma** que x é um elemento qualquer,
2. **Suponha** que $x \in A$,
3. **assim** $x = 2i, i \in \mathbb{Z}$,
4. **desde que** existe $k \in \mathbb{Z}$ tal que $k = j - 1$ e fazendo $i = k$,
5. **tem-se que** $x = 2i = 2k = 2(j-1) = 2j - 2$.
6. **Então** $x \in B$.
7. **Portanto**, Se $x \in A$, então $x \in B$.
8. **Consequentemente**, $\forall x.[$ Se $x \in A$, então $x \in B]$.
9. **Assuma** que x é um elemento qualquer,
10. **Suponha** que $x \in B$.
11. **assim** $x = 2j - 2, j \in \mathbb{Z}$,
12. **desde que** $j - 1 \in \mathbb{Z}$, pode-se fazer $i = j - 1$
13. **logo** $x = 2i$.
14. **Então** $x \in A$.
15. **Portanto**, Se $x \in B$, então $x \in A$.
16. **Consequentemente**, $\forall x.[$ Se $x \in B$, então $x \in A]$.
17. **Portanto,** $A \subseteq B$ e $B \subseteq A$ assim por definição $A = B$.

Neste momento o exemplo anterior serve apenas para esboçar a ideia de um diagrama de bloco para uma demonstração, note que fica evidente que a depender

[1]A escrita dos termos reservados em negrito em geral será usada para que o leitor consiga identificar o que é informação último da prova e o que é apenas um artificio textual para dá melhor entendimento a demonstração.

da situação alguns termos de ligação são melhores que outros, e o mesmo também é válido para os termos de inicialização e conclusão de bloco.

Aqui não será detalhando a aplicação dos métodos de demonstração usado na demonstração do Exemplo 2.1, mas nas próximas seções serão apresentados cada um dos métodos de demonstração, e seguida será gradativamente apresentados exemplos para esboçar ao leitor como é usado o diagrama de blocos e relação a cada método de demonstração.

Como o leitor pode ter notado pelo diagrama de bloco no Exemplo 2.1, é possível enxergar o diagrama como ambiente muito similar a ideia de um programa imperativo em uma linguagem de programação estruturada (como Pascal ou C), no sentido de que, uma demonstração pode ser visto como a combinação de diversos blocos, em que os blocos respeito uma hierarquia e podem está aninhados entre si, a hierarquia dos bloco é determinar por uma indentação[2].

2.2 Demonstrando Implicações

Este documento irá iniciar a apresentação dos métodos de demonstração a partir das estratégias usadas para demonstrar a implicação, isto é, as estratégias usadas para provar asserção da forma: “se α, então β”.

Definição 2.2 — Prova Direta (PD). Dado uma asserção da forma: “se α, então β”. A metodologia de prova direta para tal asserção consiste em supor α como sendo verdade e a partir disto deduzir β.

Esta estratégia é provavelmente a técnicas mais famosa e usada dentre todos os métodos de demonstração que existem, um conhecedor de lógica pode notar facilmente que tal estratégia nada mais é do que a regra de dedução natural chamada de introdução da implicação[48].

No que diz respeito ao diagrama tal estratégia consistem em: (1) criar um bloco, e dentro deste bloco na primeira linha irá conter a afirmação de que α está sendo assumido com uma hipótese verdadeira; (2) nas próximas n linhas irão acontecer as deduções necessárias até que na linha $n+2$ seja deduzido o β e o bloco é fechado e (3) na linha $n+3$ será adicionada a conclusão do bloco. A seguir serão apresentados exemplos do uso do método de demonstração direto para implicações e seu uso junto com o diagrama de bloco.

Exemplo 2.2 Será Provado a asserção, **“Se x é ímpar, então $x^2 + x$ é par”**, usando **PD**. A prova começa abrindo um bloco e inserido na primeira linha a hipótese de que o antecedente x **é um número ímpar** é verdadeira, ou seja, tem-se:

1.	**Suponha** que x é um número ímpar
2.	

em seguida pode-se na linha 2 deduzir a forma de x, mudando o diagrama para:

[2] Indentação é um termo utilizando em código fonte de um programa, serve para ressaltar, identificar ou definir a estrutura do algoritmo.

1.	**Suponha** que x é um número ímpar,
2.	**logo** $x = 2k + 1, k \in \mathbb{Z}$,
3.	

agora nas próximas duas linhas pode-se deduzir respectivamente as formas (ou valores) de x^2 e $x^2 + x$, assim o diagrama é atualizado para:

1.	**Suponha** que x é um número ímpar,
2.	**logo** $x = 2k + 1, k \in \mathbb{Z}$,
3.	**assim** $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4.	**dessa forma** $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5.	

note que $x^2 + x = 2((2k^2 + 2k) + k + 1)$ pode ser reescrito (por substituição) como $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1$, essa dedução é inserida na linha de número 5 atualizando o diagrama para:

1.	**Suponha** que x é um número ímpar,
2.	**logo** $x = 2k + 1, k \in \mathbb{Z}$,
3.	**assim** $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4.	**dessa forma** $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5.	**logo** $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$.
6.	

assim pode-se então deduzir a partir da informação na linha de número 5 que $x^2 + x$ é um número par, assim o diagrama muda para a forma:

1.	**Suponha** que x é um número ímpar,
2.	**logo** $x = 2k + 1, k \in \mathbb{Z}$,
3.	**assim** $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4.	**dessa forma** $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5.	**logo** $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$,
6.	**então** $x^2 + x$ por definição é um número par.
7.	

note porém que a informação na deduzida na linha de número 6 é exatamente o consequente da implicação que se queria deduzir. Portanto, o objetivo interno ao bloco foi atingido, pode-se então fechar o bloco introduzindo abaixo dele a conclusão do bloco, ou seja, na linha de número 7 é escrito que o antecedente de fato implica no consequente, assim o diagrama fica da forma:

1.	**Suponha** que x é um número ímpar,
2.	**logo** $x = 2k + 1, k \in \mathbb{Z}$,
3.	**assim** $x^2 = 4k^2 + 4k + 1, k \in \mathbb{Z}$,
4.	**dessa forma** $x^2 + x = 2((2k^2 + 2k) + k + 1), k \in \mathbb{Z}$.
5.	**logo** $x^2 + x = 2j$ com $j = (2k^2 + 2k) + k + 1, k \in \mathbb{Z}$,
6.	**então** $x^2 + x$ por definição é um número par.
7.	**Portanto**, Se x é ímpar, então $x^2 + x$ é par.

assim o objetivo a ser demonstrado foi atingido e, portanto, a prova está completa.

Tomando Notas 2.1 – Como justificar adequadamente! Na demonstração apresentada no Exemplo 2.2 as justificativas da evolução do diagrama fora apresentadas passo a passo e separadas do diagrama, isso foi adotado nesse primeiro exemplo para detalhar a evolução da demonstração ao leitor, entretanto, isso não é o padrão, o normal (que será adotado) é que a justificativa (caso necessário[a]) da dedução de uma linha seja inserida a direita da informação deduzida, destacada em azul. Além disso, nas justificativas das provas as palavras definição, associatividade, comutatividade serão abreviadas para DEF, ASS, COM respetivamente.

[a]Quando a justificativa for trivial, ela não será inserida na prova.

Exemplo 2.3 Demonstração da asserção: Se $x = 4k$, então x é múltiplo de 2.

1.	**Suponha** que $x = 4k, k \in \mathbb{Z}$,	Hipótese
2.	**assim** $x = (2 \cdot 2)k, k \in \mathbb{Z}$,	Reescrita da linha 1
3.	**dessa forma** $x = 2(2k), k \in \mathbb{Z}$.	ASS da multiplicação
4.	**logo** $x = 2i$, com $i = 2k, k \in \mathbb{Z}$.	Reescrita da linha 3
5.	**então** x é múltiplo de 2.	DEF de múltiplo de 2
6.	**Portanto**, Se $x = 4k$, então x é múltiplo de 2.	PD (linhas 1-6)

O leitor deve ter notado nos Exemplos 2.2 e 2.3 as demonstrações sempre iniciam das hipótese que estão sendo assumidas, isto é, os antecedentes das implicações, isso ocorrer por que nenhuma informação adicional (necessária) é apresentada como premissa, há caso entretanto, que as premissas são importantes para o desenvolvimento da prova, como será visto no próximo exemplo.

Exemplo 2.4 Demonstração da asserção: Dado m inteiro maior ou igual que 5 e n um número impar maior que 0. Se $m = 2i + 1$, então $m + n \geq 6$.

1.	$m \geq 5, m \in \mathbb{Z}$	Premissa
2.	$n = 2j + 1, j \in \mathbb{Z}^+$	Premissa
3.	**Suponha** que $m = 2i + 1$,	Hipótese
4.	**assim** $m + n = 2(i + j + 1)$	
5.	**desde que** $m \geq 5$ tem-se que $i \geq 2$,	
6.	**mas** como $n \in \mathbb{Z}_+$ tem-se que $j \geq 0$,	
7.	**assim** $i + j + 1 \geq 3$,	Direto das linhas 5 e 6
8.	**logo** $2(i + j + 1) \geq 6$	
9.	**então** $m + n \geq 6$.	Reescrita da linha 8
10.	**Portanto**, Se $m = 2i + 1$, então $m + n \geq 6$.	PD (linhas 3-9)

Exemplo 2.5 Demonstração da asserção: Dado $m, n \in \mathbb{R}$ e $3m + 2n \leq 5$. Se $m > 1$, então $n < 1$.

1.	$m, n \in \mathbb{R}$	Premissa
2.	$3m + 2n \leq 5$	Premissa
3.	**Suponha** que $m > 1$,	Hipótese
4.	**assim** $3m > 3$,	
5.	**desde que** $3m \leq 5 - 2n$,	
6.	**tem-se que** $3 < 3m \leq 5 - 2n$	Direto das linhas 4 e 5
7.	**logo** $3 < 5 - 2n$,	
8.	**assim** $3 + 2n < 5$,	
9.	**então** $n < 1$.	
10.	**Portanto**, Se $n > 1$, então $n < 1$.	PD (linhas 3-10)

Além do método de prova direta asserções que são implicações podem ser provadas por um segundo método, chamado método da contrapositiva (ou contraposição). Como dito em [52], o método da contrapositiva se baseia na equivalência semântica[3] da expressão "Se α, então β" com a expressão "Se não β, então não α". Formalmente o método de demonstração por contrapositiva é como se segue.

Definição 2.3 — Prova por contrapositiva (PCP). Dado uma asserção da forma: "se α, então β". A metodologia de prova por contrapositiva para tal asserção consiste em demonstrar usando PD a asserção "se não β, então não α", em seguida concluir (ou enunciar) que a veracidade de "se α, então β" segue da veracidade de "se não β, então não α".

Agora em termos do diagrama de blocos o método PCP apresenta o seguinte raciocínio de construção do diagrama: (1) abrir um bloco com a primeira linha em branco; (2) realizar em um bloco (interno) a demonstração de que "se não β, então não α" e (3) após a conclusão deste segundo bloco, o primeiro bloco é fechado, e sua conclusão consiste na informação "se α, então β" e a justificativa de tal informação é simplesmente a conclusão PCP das linhas i-j, onde i-j diz respeito ao intervalo contendo as linhas do bloco e da conclusão da prova de "se não β, então não α".

Observação 2.2 — Apenas organização! ALiCIA se irrita fácil com escritas que ela acha feia, então ela quer tudo sempre organizadinho, assim vale salientar que a linha em branco no início do próximo exemplo é apenas um **fator estético** adotado para agradar ela, para tornar a leitura do diagrama da demonstração mais agradável. Esse recurso pode voltar a ser usado em exemplos futuros. Além disso, ela acha que é mais conveniente escrever, por exemplo apenas $l2$, do que ter que escrever linhas 2 nas justificativas, assim o l nas justificativas a partir deste ponto deve ser lido como "linha" ou "linhas" no caso de ser $lx - y$ onde x e y são os números.

[3] Para um entendimento sobre equivalência semântica ver [21, 33].

Exemplo 2.6 Demonstração da asserção: Se $n! > (n+1)$, então $n > 2$.

1.		
2.	**Suponha** que $n \leq 2$,	Hipótese
3.	**assim** $n = 0, n = 1$ ou $n = 2$	Direto da $l2$
4.	**logo** $n! = 1$ ou $n! = 2$,	Da $l3$ e da DEF de fatorial
5.	**então** $n! \leq (n+1)$ com $n \leq 2$.	Direto de $l3$ e $l4$
6.	**Portanto**, Se $n \leq 2$, então $n! \leq (n+1)$.	PD $(l2 - 5)$
7.	**Por contrapositiva**, Se $n! > (n+1)$, então $n > 2$.	PCP $(l2 - 6)$

Exemplo 2.7 Demonstração da asserção: Se $n \neq 0$, então $n + c \neq c$.

1.		
2.	**Suponha** que $n + c = c$,	Hipótese
3.	**assim** $n + c - c = c - c$	
4.	**logo**, $n + 0 = 0$,	
5.	**então** $n = 0$.	
6.	**Portanto**, Se $n + c = c$, então $n = 0$.	PD $(l2 - 5)$
7.	**Logo por contrapositiva**, Se $n \neq 0$, então $n + c \neq c$.	PCP $(l2 - 6)$

Exemplo 2.8 Demonstração da asserção: Dado três números $x, y, z \in \mathbb{R}$ com $x > y$. Se $xz \leq yz$, então $z \leq 0$.

1.	$x, y, z \in \mathbb{R}$,	Premissa
2.	$x > y$,	Premissa
3.		
4.	**Suponha** que $z > 0$,	Hipótese
5.	**então** $xz > yz$,	Das $l2$ e $l4$ e da MON[a] da $\cdot$ em $\mathbb{R}$
6.	**Portanto**, Se $z > 0$, então $xz > yz$.	PD ($l2$-5)
7.	**Por contrapositiva**, Se $xz \leq yz$, então $z \leq 0$.	PCP $(l3 - 6)$

[a]MON aqui é a abreviatura de monotonicidade.

Exemplo 2.9 Demonstração da asserção: Se n^2 é par, então n é par.

1.		
2.	**Suponha** que n não é par,	Hipótese
3.	**logo** $n = 2k + 1$ com $k \in \mathbb{Z}$,	DEF de paridade
4.	**assim** $n^2 = 4k^2 + 4k + 1$ com $k \in \mathbb{Z}$,	
5.	**dessa forma** $n^2 = 2j + 1$ com $j = 2k^2 + 2k$,	Reescrita de $l4$
6.	**então** n^2 não é par	DEF de paridade
7.	**Portanto**, Se n não é par, então n^2 não é par.	PD ($l2$-6)
8.	**Logo por contrapositiva**, Se n^2 é par, então n é par.	PCP ($l2$-6)

2.3 Demonstração por Absurdo

O método de demonstração por redução ao absurdo[4] (ou por contradição) tem por objetivo provar que a asserção α junto com as premissas (se houverem) é verdadeira a partir da prova de que a suposição de que a asserção "não α" seja verdadeira junto das mesmas premissas (mencionadas anteriormente) gera um absurdo (ou contradição). O fato deste absurdo seja gerado, permite concluir que suposição de que a asserção "não α" seja verdadeira é ridícula, ou seja, "não α" tem que ser falsa e, portanto, a asserção α tem que ser verdadeira.

Definição 2.4 — Prova por Redução ao Absurdo (RAA). A metodologia para uma demonstração por redução ao absurdo de uma asserção α, consiste em supor que não α é uma hipótese verdadeira, então deduzir um absurdo (ou contradição). Em seguida concluir que dado que a partir de não α foi produzido um absurdo pode-se afirma que α é verdadeiro.

Em termos do diagrama de blocos o método RAA consiste nos seguintes passo: (1) abrir um bloco cuja primeira linha é vazia; (2) iniciar um bloco interno em que na primeira linha deste bloco o termo de inicialização do bloco (já listados anteriormente) é seguida da expressão "por absurdo" e da asserção não α; (3) em seguida nas próximas n linhas irão acontecer as deduções necessárias até que na linha $n + 2$ seja deduzido o absurdo (ou uma contradição) e o bloco é fechado, inserido na linha $n + 3$ a informação de que "Se não α, então $\perp$" e é fechado o bloco externo e (4) na linha $n + 4$ será adicionada a conclusão do bloco externo, contendo algo como " Portanto, α é verdadeiro".

Tomando Notas 2.2 – Representação do absurdo Aqui como em muitos outros materiais será usado o símbolo $\perp$[a] para denotar o absurdo.

[a] Este símbolo também costuma ser usado na teoria de reticulados para representar o bottom nos reticulados.

Tomando Notas 2.3 – Sobre provar usando RAA! O leitor um pouco mais atento perceberá que provar o asserção P usando RAA, é na verdade, realizar uma demonstração para uma asserção da seguinte forma $\neg P \Rightarrow \perp$.

[4] *Reductio ad absurdum* em latim.

Exemplo 2.10 Demonstração da asserção: $\sqrt{2} \notin \mathbb{Q}$.

1.		
2.	**Assuma por absurdo** que $\sqrt{2} \in \mathbb{Q}$,	Hipótese
3.	**logo** existem $a, b \in \mathbb{Z}$ tal que $\sqrt{2} = \frac{a}{b}$ e $mdc(a, b) = 1$	
4.	**logo** $a^2 = 2b^2$, ou seja, a^2 é par,	
5.	**dessa forma** $a = 2i$ com $i \in \mathbb{Z}$,	De $l4$ e do Exemplo 2.9
6.	**logo** $b^2 = 2i^2$ com $i \in \mathbb{Z}$,	
7.	**dessa forma** $b = 2j$ com $j \in \mathbb{Z}$,	De $l6$ e do Exemplo 2.9
8.	**assim** $mdc(a, b) \geq 2$,	De $l5$ e $l7$
9.	**mas** $mdc(a, b) = 1$ e $mdc(a, b) \geq 2$ é um absurdo.	Direto de $l3$ e $l8$
10.	**Portanto**, Se $\sqrt{2} \in \mathbb{Q}$, então $\bot$.	PD ($l2$-10)
11.	**Consequentemente**, $\sqrt{2} \notin \mathbb{Q}$.	RAA ($l2$-11)

Tomando Notas 2.4 – O que realmente uma RAA? ALiCIA precebeu que internamente a prova por redução ao absurdo de uma asserção α, deve ser demonstrado a asserção: $(\neg\alpha) \Rightarrow \bot$. Isso é interessante não é?

Exemplo 2.11 Demonstração da asserção: Não existe solução inteira positiva não nula para a equação diofantina[a] $x^2 - y^2 = 1$.

1.		
2.	**Assuma por absurdo** $\exists x, y \in \mathbb{Z}_+^*$ com $x^2 - y^2 = 1$,	Hipótese
3.	**assim** $min(x, y) = 1$ e $(x - y)(x + y) = 1$,	
4.	**logo** $x - y = x + y = 1$ ou $x - y = -1$ e $x + y = -1$,	Por $x, y \in \mathbb{Z}_+^*$
5.	**com** $x - y = 1$ e $x + y = 1$ tem-se $x = 1$ e $y = 0$,	
6.	**assim** $min(x, y) \neq 1$,	De $l5$
7.	**com** $x - y = -1$ e $x + y = -1$ segue $x = -1$ e $y = 0$,	
8.	**assim** $min(x, y) \neq 1$,	De $l7$
9.	**mas** $min(x, y) = 1$ e $min(x, y) \neq 1$ é um absurdo.	De $l3, l6$ e $l8$.
10.	**Portanto**, Se $\exists x, y \in \mathbb{Z}_+^*$ tal que $x^2 - y^2 = 1$, então $\bot$.	PD ($l2$-10)
11.	**Portanto**, não $\exists x, y \in \mathbb{Z}_+^*$ tal que $x^2 - y^2 = 1$.	RAA ($l2$-10)

[a] Equações diofantinas são equações polinomiais, que permite a duas ou mais variáveis assumirem apenas valores inteiros.

Equações diofantinas tem papel central para computação, assim vale mencionar aqui que um importante resultado sobre essas equações, e que possui forte impacto computabilidade, foi demonstrado pelos trabalhos de Julia Robinson (1919–1985) e Yuri Matiyasevich(1947–.) [49]. Tal resultado solucina o décimo problema da lista de Hilbert[5], de forma sucinta o resultado diz que não existe um algoritmo universal para determinar se uma equação diofantina tem raízes inteiras.

[5] Apresentada pelo matemático alemão David Hilbert (1862–1943).

Exemplo 2.12 Demonstração da asserção: Se $3n + 2$ é ímpar, então n é ímpar.

1.		
2.	**Suponha por absurdo** que $3n + 2$ é ímpar e n é par,	Hipótese
3.	**logo** $n = 2k, k \in \mathbb{Z}$,	DEF de paridade
4.	**dessa forma** $3n + 2 = 2(3k + 1), k \in \mathbb{Z}$,	
5.	**assim** $3n + 2$ é par,	DEF de paridade
6.	**mas** $3n + 2$ ser ímpar e $3n + 2$ ser par, é um absurdo.	De $l2$ e $l5$
7.	**Portanto**, se $3n + 2$ é ímpar e n é par, então $\perp$.	PD ($l2$-7)
8.	**Portanto**, se $3n + 2$ é ímpar, então n é ímpar.	RAA ($l2$-8)

2.4 Demonstrando Generalizações

Antes de falar sobre o método usado para demonstrar generalizações deve-se primeiro reforçar ao leitor o que é são generalizações. Uma generalização é qualquer asserção que contenha em sua formação expressões das formas:

(a) Para todo ________.

(b) Para cada ________.

(c) Para qualquer ________.

Exemplo 2.13 A seguintes asserções são generalizações.

(a) Todos os cachorros são mamíferos.

(b) Todos os números inteiros possuem um inverso aditivo.

(c) Todos os times de futebol pernambucanos são times brasileiros.

Nos termos da lógica uma asserção é uma generalização sempre que o quantificador universal é o quantificador mais externo a da asserção. Agora que o leitor está a par do que é uma generalização, pode-se prosseguir o texto deste documento apresentando formalmente o método de demonstração para generalizações.

Definição 2.5 — Prova de Generalizações (PG). Para provar uma asserção da forma, "$(\forall x)[P(x)]$", em que $P(x)$ é uma asserção acerca da variável x. Deve-se assumir que a variável x assume como valor um objeto qualquer no universo do discurso de que trata a generalização, em seguida, provar que a asserção $P(x)$ é verdadeira, usando as propriedades disponível de forma genérica para os objetos do universo do discurso.

Em termos do diagrama, a prova de uma generalização começa inserido na primeira linha de um bloco a informação de que x é um objeto genérico (ou qualquer) do discurso, em seguida deve ser provado $P(x)$ é verdadeiro, caso seja necessário deve ser é aberto um novos blocos para as subprovas, após demonstrar que $P(x)$ é verdadeiro para um x genérico do discurso, o bloco externo (aberto para a prova da generalização) é fechado e pode-se apresentar a conclusão de que todo objeto x do discurso $P(x)$ é verdadeiro. Note que esse raciocínio de demonstração garante (com explicado em [72]) que a asserção P é universal sobre o universo do discurso, ou seja, garante a universalidade da asserção P.

Exemplo 2.14 Demonstração da asserção: $(\forall x \in \{4n \mid n \in \mathbb{N}\})[x \text{ é par}]$.

1.	**Assuma** que $x \in \{4n \mid n \in \mathbb{N}\}$	Hipótese
2.	**dessa forma** $x = 4n, n \in \mathbb{N}$,	DEF do discurso
3.	**logo** $x = (2 \cdot 2)n, n \in \mathbb{N}$,	Reescrita de $l2$
4.	**dessa forma** $x = 2(2n), n \in \mathbb{N}$,	ASS da $\cdot$
5.	**assim** $x = 2k, k \in \mathbb{N}$,	
6.	**então** x é par.	DEF de paridade
7.	**Portanto**, com $x \in \{4n \mid n \in \mathbb{N}\}$, tem-se que x é par.	
8.	**Consequentemente**,$(\forall x \in \{4n \mid n \in \mathbb{N}\})[x \text{ é par}]$.	PG ($l1$-7)

Exemplo 2.15 Demonstração da asserção: $(\forall X, Y \subseteq \mathbb{U})[\text{se } X \neq \emptyset, \text{ então } (X \cup Y) \neq \emptyset]$.

1.	**Considere** dois conjuntos quaisquer $X, Y \subseteq \mathbb{U}$	Hipótese
2.	**Suponha** que $X \neq \emptyset$,	Hipótese
3.	**logo** existe pelo menos um $x \in X$,	
4.	**desde que** $x \in X$ tem-se que $x \in (X \cup Y)$,	
5.	**então** $(X \cup Y) \neq \emptyset$.	
6.	**Consequentemente**, Se $X \neq \emptyset$, então $X \cup Y \neq \emptyset$.	PD ($l2$-5)
7.	**Portanto**,$(\forall X, Y \subseteq \mathbb{U})[\text{se } X \neq \emptyset, \text{ então } (X \cup Y) \neq \emptyset]$.	PG ($l1$-6)

Um erro que muitos iniciantes frequentemente cometem ao tentar provar enunciados de generalização é utilizar uma (ou mais) propriedade(s) de um elemento genérico x para provar $P(x)$, entretanto esta(s) propriedade(s) usada(s) não é (são) compartilhada(s) por todos os elementos de $\mathbb{U}$, isto é, apenas um subconjunto de $\mathbb{U}$ apresenta a(s) propriedade(s) usadas, para mais detalhes sobre este tipo de erro podem ser consultados em [72].

Exemplo 2.16 Demonstração da asserção: $(\forall n \in \mathbb{Z})[\text{se } n > 2, \text{ então } n^2 > n + n]$.

1.	**Assuma** que n é um número inteiro,	Hipótese
2.	**Suponha** que $n > 2$,	Hipótese
3.	**logo** $n \cdot n > 2x$,	MON[a] da $\cdot$ em $\mathbb{Z}$
4.	**então** $n^2 > n + n$.	Reescrita de $l3$
5.	**Dessa forma**, se $n > 2$, então $x^2 > n + n$.	PD ($l2$-4)
6.	**Portanto**,$(\forall n \in \mathbb{Z})[\text{se } n > 2, \text{ então } x^2 > n + n]$.	PG ($l1$-5)

[a] Como antes MON significa monotonicidade.

Exemplo 2.17 Prova da asserção: Dado $(\forall n \in \mathbb{Z})[3(n^2 + 2n + 3) - 2n^2 \text{ é um quadrado perfeito}]$.

1.	**Assuma** que n é um número inteiro,	Hipótese
2.	**Desde que** $3(n^2 + 2n + 3) - 2n^2 = 3n^2 + 6n + 9 - 2n^2$,	
3.	**mas** $3n^2 + 6n + 9 - 2n^2 = n^2 + 6n + 9$,	
4.	**assim** $3(n^2 + 2n + 3) - 2n^2 = n^2 + 6n + 9$	De $l2$ e $l3$
5.	**mas** $n^2 + 6n + 9 = (n + 3)^2$,	
6.	**logo** $3(n^2 + 2n + 3) - 2n^2 = (n + 3)^2$,	
7.	**Dessa forma**, $3(n^2 + 2n + 3) - 2n^2$ é um quadrado perfeito.	Direto de $l2$-6
8.	**Portanto**,$(\forall n \in \mathbb{Z})[3(n^2 + 2n + 3) - 2n^2$ é um quadrado perfeito].	PG ($l1$-7)

2.5 Demonstrando Existência e Unicidade

Antes de falar sobre o método de demonstração existencial deve-se primeiro reforçar ao leitor o que é um enunciado existencial. Um enunciado de uma sentença do tipo existencial é qualquer asserção que inicia usando as expressões das forma seguir:

(a) Existe um(a) ________.

(b) Há um(a) ________.

Agora sobre a metodologia para demonstrar (provar) a existência de um objeto com um determinada propriedade, ou seja, provar que um certo objeto x satisfaz uma propriedade P, é especificada pela definição a seguir.

Definição 2.6 — Prova de existência (PE). Para provar uma asserção da forma "$(\exists x)[P(x)]$", em que $P(x)$ é uma asserção sobre a variável x. Deve-se exibir[a] um elemento específico "a" pertencente ao universo do discurso, e mostrar que a asserção $P(x)$ é verdadeira quando x é instanciado como sendo exatamente o elemento a, ou seja, deve-se mostrar que $P(a)$ é verdadeira.

[a]Ou seja, deve-se instanciar o x para algum objeto concreto do discurso.

Em relação ao diagrama de bloco, uma demonstração de existência, isto é, uma prova de uma asserção $(\exists x)[P(x)]$, irá se comportar de forma muito semelhante a uma demonstração de generalidade, as única mudanças significativas é que tal método inicia seu bloco com a declaração de que será atribuído um objeto **específico** em vez de considerar a variável genérica a x, ou seja, é realizado uma instanciação de um elemento. Além disso, a conclusão do bloco externo deve ser exatamente a $(\exists x)[P(x)]$, ou seja, a conclusão deverá ser a asserção existencial.

Exemplo 2.18 Demonstração da asserção: $(\exists n \in \mathbb{N})[n = n^2]$.

1.	**Deixe ser** $n = 1$	Instanciação
2.	**logo** $n \cdot n = 1 \cdot n$,	MON de $\cdot$ em $\mathbb{N}$
3.	**assim** $n^2 = n$,	Reescrita da $l2$
4.	**então** $n = n^2$,	Reescrita da $l3$
5.	**Portanto**,$(\exists n \in \mathbb{N})[n = n^2]$.	PE ($l1$-4)

Exemplo 2.19 Demonstração da asserção: $(\exists a, b \in \mathbb{I})[m^n \in \mathbb{Q}]$.

1.	**Deixe ser** $a = \sqrt{2}$ e $b = \sqrt{2}$	Instanciação
2.	**logo** $a, b \in \mathbb{I}$,	Do Exemplo 2.10
3.	**Se** $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$,	
4.	**então** não há mais nada a ser demonstrado.	
5.	**Consequentemente**, se $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, então $a^b \in Q$.	PD de $l3$-4
6.	**Se** $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$,	
7.	**logo** $\sqrt{2}^{\sqrt{2}} \in \mathbb{I}$,	
8.	**assim** fazendo $c = a^b$ tem-se que $c \in \mathbb{I}$,	
9.	**então** $c^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$.	
10.	**Portanto**, se $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, então $c^b \in \mathbb{Q}$ com $c \in \mathbb{I}, c = a^b$.	PD de $l6$-9
11.	**Portanto**,$(\exists m, n \in \mathbb{I})[m^n \in \mathbb{Q}]$.	PE ($l1$-10)

Exemplo 2.20 Demonstração da asserção: $(\exists X \subseteq \mathbb{U})[(\forall Y \subseteq \mathbb{U})[X \cup Y = Y]]$.

1.	**Deixe ser** $X = \emptyset$,	Instanciação
2.	**Assuma** que $Y \subseteq \mathbb{U}$	Hipótese
3.	**logo** $y \in Y$ tem-se que $y \in (\emptyset \cup Y)$	DEF de união
4.	**assim** $Y \subseteq (X \cup Y)$,	De $l1$ e $l3$
5.		
6.	**Suponha por absurdo** que $(\emptyset \cup Y) \nsubseteq Y$	Hipótese
7.	**assim** tem-se que existe $z \in (\emptyset \cup Y)$ e $z \notin Y$,	
8.	**dessa forma** $z \in \emptyset$,	De $l7$
9.	**desde que** $X = \emptyset$ é um absurdo que $z \in X$,	De $l1$ e da DEF de $\emptyset$
10.	**Portanto**, se $(X \cup Y) \nsubseteq Y$, então $\perp$.	Conclusão da PD ($l6$-9)
11.	**Consequentemente**, $(X \cup Y) \subseteq Y$.	Conclusão RAA ($l6$-10)
12.	**Dessa forma**, $(X \cup Y) = Y$.	Direto de $l4$ e $l11$
13.	**Portanto**,$(\exists X \subseteq \mathbb{U})[(\forall Y \subseteq \mathbb{U})[X \cup Y = Y]]$.	PE ($l1$-12)

O leitor que leu com atenção o Capítulo 1, ou que tenha domínio sobre a teoria dos conjuntos sabe que $(\emptyset \cup X) = X$, para qualquer conjunto X, assim poderia escrever uma prova bem mais curta (fica como exercício) do que a demonstração mostrada no Exercício 2.20.

Agora vale ressaltar uma importante questão, a prova de existência não garante que um único elemento do discurso satisfaça uma determinada propriedade, note que no Exemplo 2.18 poderia ser substituído 1 pelo número natural 0 sem haver qualquer perca para a demonstração.

De fato, o que a prova de existência garante é que **pelo menos um** elemento dentro do discurso satisfaz a propriedade que está sendo avaliada. Uma demonstração que garante que **um e apenas um** elemento em todo discurso satisfaz uma certa propriedade é chamada de demonstração de unicidade.

Antes de falar sobre o método de demonstração de unicidade deve-se primeiro reforçar ao leitor o que é um enunciado existencial de unicidade. Basicamente tal tipod e enunciado consiste de um enunciado de existência que adiciona os termos "único" ou "apenas um" na uma sentença do tipo existencial ficando da formas:

(a) Existe apenas um(a) ________.

(b) Há apenas um(a) ________.

(c) Há somente um(a) ________.

ou ainda,

(a) Existe um(a) único(a) ________.

(b) Há um(a) único(a) ________.

Tomando Notas 2.5 – Simbologia Deste ponto em diante sempre que possível será substituido a escrita "se P, então Q" pela notação da lógica simbólica $P \Rightarrow Q$.

Definição 2.7 — Prova de unicidade (PU). Uma prova de unicidade consiste em provar uma asserção da forma "$(\exists x)[P(x) \wedge (\forall y)[P(y) \Rightarrow x = y]]$", em que P é uma asserção sobre os elementos do discurso. Para tal primeiro deve-se demonstrar que a asserção "$(\exists x)[P(x)]$" é verdadeira, e depois prova que a generalização $(\forall y)[P(y) \Rightarrow x = y]$ também é verdadeira.

Com respeito ao diagrama de blocos, uma demonstração de unicidade apresenta um diagrama similar ao de uma prova de existência, entretanto, internamente ao bloco da demonstração irá existir uma subprova para a asserção $(\forall y)[P(y) \Rightarrow x = y]$, sendo está subprova responsável pro mostrar a unicidade. Por fim após fechar o bloco mais externo deve-se enunciar a conclusão.

Tomando Notas 2.6 – Um forma curta de escrever! Como [48] é comum representar a unicidade como $(\exists! x)[P(x)]$ em vez de $(\exists x)[P(x) \wedge (\forall y)[P(y) \Rightarrow x = y]]$.

Exemplo 2.21 Demonstração da asserção: $(\exists! x \in \mathbb{N})[x+x = x \wedge (\forall y \in \mathbb{N})[y+y = y \Rightarrow x = y]]$.

1.	**Deixe ser** $x = 0$,	Instanciação
2.	**logo** $x + 0 = 0 + 0$,	
3.	**assim** $x + 0 = 0$,	
4.	**dessa forma** $x + x = x$.	De $l1$ e $l3$
5.	**Suponha** que $y \in \mathbb{N}$,	Hipótese
6.	**Assuma** que $y + y = y$,	Hipótese
7.	**logo** $y = y - y$,	
8.	**assim** $y = 0$,	
9.	**então** $y = x$,	Reescrita de $l8$
10.	**Consequentemente**,$y + y = y \Rightarrow x = y$.	PD ($l6$-9)
11.	**Portanto**,$(\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]$,	PG ($l5$-10)
12.	**logo** $x + x = x \wedge (\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]$.	Direto de $l4$ e $l11$
13.	**Portanto**,$(\exists x \in \mathbb{N})[x + x = x \wedge (\forall y \in \mathbb{N})[y + y = y \Rightarrow x = y]]$.	PU ($l2$-13)

Exemplo 2.22 Demonstração da asserção: $(\forall x \in \mathbb{Z})[(\exists! y \in \mathbb{Z})[x + y = 0]]$.

1.	**Assuma** que $x \in \mathbb{Z}$,	Hipótese
2.	**Deixe ser** $y = -x$,	Instanciação
3.	**logo** $x + y = x + (-x)$,	
4.	**mas** $x + (-x) = 0$,	
5.	**então** $x + y = 0$.	
6.	$(\exists y \in \mathbb{Z})[x + y = 0]$.	PE ($l2$-5)
7.	**Assuma** que $z \in \mathbb{Z}$,	Hipótese
8.		
9.	**Suponha por absurdo** que $x + z = 0$ e $z \neq y$,	Hipótese
10.	**desde que** $x + y = 0$ tem-se que $x + z = x + y$,	
11.	**mas** assim $z = y$, o que contradiz é um absurdo.	
12.	**Consequentemente**, se $x + z = 0$ e $z \neq -x$, então $\perp$.	PD ($l8$-10)
13.	**Portanto**, se $x + z = 0$, então $x = y$.	RAA ($l8$-11)
14.	**Dessa forma** $(\forall z \in \mathbb{Z})[x + z = 0 \Rightarrow z = y]$.	PG ($l7$-13)
15.	**Portanto**,$(\forall x \in \mathbb{Z})[(\exists! y \in \mathbb{Z})[x + y = 0]]$.	PU ($l2$-13)

2.6 Demonstração Guiada por Casos

Para realizar uma demonstração guiada por casos (ou simplesmente demonstração por casos) a estratégia emprega consiste em demonstrar cobrindo todos os casos possíveis que as premissas α_i em um enunciado podem assumir, formalmente esta metodologia de demonstração é definida como se segue.

Definição 2.8 — Prova por Casos (PPC). Uma prova por caso, consiste em provar um enunciado da forma: Se α_1 ou $\cdots$ ou α_n, então β. Para isso é realizado os seguintes passos:

- Supor α_1 (e apenas ela) verdadeira, e demonstrar β.

  $\vdots$

- Supor α_n (e apenas ela) verdadeira, e demonstrar β.

Com respeito ao diagrama de blocos uma prova por casos consiste de um diagrama que possui em seu interior n provas da forma $\alpha_i \Rightarrow \beta$ com $1 \leq i \leq n$, após todas as sub-provas serem apresentadas a última linha no diagrama mais externo irá expressar uma sentença da forma $(\alpha_1 \Rightarrow \beta) \wedge \cdots \wedge (\alpha_n \Rightarrow \beta)$, então o diagrama será fechado e será escrita a conclusão do diagrama. O exemplo a seguir ilustram esse procedimento.

Exemplo 2.23 Demonstração da asserção: Dado $n \in \mathbb{N}$. Se $n \leq 2$, então $n! \leq n+1$.

1.	$n \in \mathbb{N}$	— Premissa
2.	**Assuma** que $n = 0$,	Hipótese
3.	**desde que** $0! = 1$	
4.	**assim** $0! \leq 1$	
5.	**mas** $1 = n + 1$	
6.	**então** $n! \leq n + 1$	
7.	**Portanto**, se $n = 0,$ então $n! \leq n + 1$	PD $(l2 - 5)$
8.	**Assuma** que $n = 1$,	Hipótese
9.	**desde que** $n! = 1$	
10.	**assim** $n! < 2$	
11.	**mas** $2 = n + 1$	
12.	**então** $n! < n + 1$	
13.	**Portanto**, se $n = 1,$ então $n! < n + 1$	PD $(l7 - 11)$
14.	**Assuma** que $n = 2$,	Hipótese
15.	**desde que** $n! = 2$	
16.	**logo** $n! < 3$	
17.	**mas** $3 = n + 1$	
18.	**então** $n! < n + 1$	
19.	**Portanto**, se $n = 2,$ então $n! < n + 1$	PD $(l7 - 11)$
20.	**Portanto**, Dado $n \in \mathbb{N}$. Se $n \leq 2$, então $n! \leq n + 1$.	PPC $(l1 - 19)$

Exemplo 2.24 Demonstração da asserção: Se $x \in \mathbb{Z}$, então x^2 tem a mesma paridade de x.

1.		
2.	**Assuma** que $x = 2i$ com $i \in \mathbb{Z}$,	Hipótese
3.	**logo** $x^2 = 2(2i^2)$, com $i \in \mathbb{Z}$	
4.	**então** x é par	DEF de paridade
5.	**Portanto**, se x é par, então , x^2 é par	PD $(l2 - 4)$
6.	**Assuma** que $x = 2i + 1$ com $i \in \mathbb{Z}$,	Hipótese
7.	**logo** $x^2 = 4i^2 + 4i + 1$, com $i \in \mathbb{Z}$	
8.	**assim** $x^2 = 2(2i^2 + 2i) + 1$, com $i \in \mathbb{Z}$	Reescrita
9.	**então** x^2 é impar	DEF de paridade
10.	**Portanto**, se x é ímpar, então , x^2 é impar	PD $(l6 - 9)$
11.	**Portanto**, se $x \in \mathbb{Z},$ então x^2 tem a mesma paridade que x.	PPC $(l1 - 10)$

2.7 Outras Formas de Representação de Provas

Durante este capítulo foram apresentadas diversas metodologias para se realizar demonstrações, e para representar as provas (demonstrações) usando tais metodologias foi empregado o uso de representação por diagrama de blocos. Este documento utilizou-se dessa representação por ela ser mais amigável ao leitor iniciante na tarefa de provar teoremas.

Existem diversas outras formas de representar a demonstração de um teorema, por exemplo, o professor Thanos Tsouanas em seu livro [71], usa o conceito de tabuleiro do "jogo"da demonstração para representar as demonstrações. Por fim, vale destacar a representação das demonstrações por meio de texto formal, que consiste basicamente em descrever a prova usando um texto utilizando o máximo de formalismo matemático possível, o exemplo a seguir ilustra a representação em texto formal.

Exemplo 2.25 A representação por texto formal da demonstração da asserção: "Se n é par, então n^2 é par", pode ser da seguinte forma.

Demonstração. Suponha que n é par, logo $n = 2k$ para algum $k \in \mathbb{Z}$, dessa forma tem-se que $n^2 = n \cdot n = 2k \cdot 2k = 4k^2 = 2(2k^2)$, mas desde que a multiplicação e potenciação são fechadas em $\mathbb{Z}$ tem-se que existe $r \in \mathbb{Z}$ tal que $r = 2k^2$ e, portanto, $n^2 = 2r$, consequentemente, n^2 é par. □

A representação por texto formal é em geral a maneira utilizada de fato no meio acadêmico, para mais exemplos dessa representação veja [18, 19, 22, 53, 61] e com texto em inglês é sugerido a leitura de [63, 72]. A partir deste ponto será adotado a escrita de demonstração em texto formal, ficando assim a representação por bloco "confinada" as seções anteriores deste capítulo.

2.8 Demonstração de Suficiência e Necessidade

Na matemática (em também na computação) é comum encontrar enunciados (sejam proposições, lemas, teoremas ou propriedades de programas) da forma: "P se, e somente se, Q". Provar esse tipo de enunciado consiste em provar duas sentenças implicativas em separado, sendo elas: "Se P, então Q" e "Se Q, então P". A primeira sentença recebe o nome de **condição suficiente**, sua prova costuma ser rotulada no texto formal da demonstração por $(\Rightarrow)$. Já a segunda implicação é nomeada como **condição necessário** e na demonstração sua prova é geralmente rotulada por $(\Leftarrow)$. A seguir serão apresentados alguns exemplos de demonstrações deste tipo.

Exemplo 2.26 Considere a seguinte sentença sobre números inteiros:

"n é par se, e somente se, n^2 é par".

para demonstrar tal afirmação como mencionada anteriormente é necessário provar as condições: suficiente e necessária, a seguir é apresentado como isso será feito.

Demonstração. (⇒) A condição suficiente é trivialmente uma conclusão obtida direta do Exemplo 2.24. (⇐) A prova da condição necessária foi realizada no Exemplo 2.9. □

Exemplo 2.27 Considere a seguinte sentença sobre números inteiros:

"x é divisível por 6 se, e somente se, x é divisível por 2 e por 3".

como no exemplo anterior para demonstrar tal afirmação é preciso provar as condições, suficiente e necessária, de forma separada, e isto é feito a seguir.

Demonstração. (⇒) Suponha que x é divisível por 6, logo existe um $i \in \mathbb{Z}$ tal que $x = 6i$, mas deste que i é um inteiro podemos reescrever x como $x = 2(3i)$ e $x = 3(2i)$, agora fazendo $j = 3i$ e $k = 2i$ tem-se que $x = 2j$ e $x = 3k$ e, portanto, por definição x é divisível por 2 e por 3. (⇐) Suponha que x é divisível por 2 e por 3, ou seja, existem $i, j \in \mathbb{Z}$ tal que $x = 2i$ e $x = 3j$, mas disso tem-se que x é par e assim por transitividade da igualdade $3j$ também é par, e disso pode-se concluir que j é um número par (a prova disso fica como exercício ao leitor), dessa forma tem-se que $j = 2n$ para algum $n \in \mathbb{Z}$ e, assim tem-se que, $x = 3j = 3(2n) = 6n$, consequentemente, x é divisível por 6. □

Exemplo 2.28 Considere a seguinte sentença sobre conjuntos:

"$X \cup Y \neq \emptyset$ se, e somente se, $X \neq \emptyset$ ou $Y \neq \emptyset$".

como no exemplo anterior para demonstrar tal afirmação é preciso provar as condições, suficiente e necessária, de forma separada, e isto é feito a seguir.

Demonstração. (⇒) Suponha que $X \cup Y \neq \emptyset$, logo existe um a tal que $a \in X \cup Y$, mas pela definição de união tem-se que $a \in X$ ou $a \in Y$ e, portanto, $X \neq \emptyset$ ou $Y \neq \emptyset$. (⇐) Trivial, ficando com exercício ao leitor. □

Tomando Notas 2.7 – Nomenclatura! Em alguns textos [71, 8] a condição suficiente é chamada de "ida". Por sua vez, a condição necessária é chamada de "volta".

2.9 Refutações

Nas seções anteriores foi trabalhada a seguinte problemática: "Dada uma asserção, prove que ela é verdadeira", Agora este texto irá atacar a problemática inversa, ou seja, "Dada uma asserção, prove que ela é falsa". Resolver este tipo de problema consiste em encontrar uma refutação para a asserção.

Como antes no caso da apresentação dos métodos de demonstração nas seções anteriores, este texto irá dividir a apresentação das técnicas de refutação caso a caso, entretanto, em uma ordem diferente da que foi usada para apresentar os métodos de demonstração, para se torna mais didática ao leitor iniciante.

O método para conseguir **refutar uma asserção universal** consiste em encontrar um x no domínio do problema para o qual a propriedade (ou afirmação) exposta pela asserção não é válida, este tipo de técnica costuma ser chamada de **refutação por contraexemplo** [31], a seguir são apresentados uma série de exemplos sobre tal técnica.

Tomando Notas 2.8 – Pontução é importante! Para diferenciar uma refutação de uma demonstração, será adotada nesta seção a estratégia de terminar o argumento da refutação usando o símbolo ■ em oposição ao símbolo do túmulo de Halmos usado ao final das demonstrações.

Exemplo 2.29 Considere a asserção: $(\forall n \in \mathbb{N})[n + n > n]$.

Refutação. Considere n sendo instanciado com valor 0, mas é claro que $0 + 0 = 0$ e, portanto, 0 é um contraexemplo que refuta a asserção, $(\forall n \in \mathbb{Z})[n+n > n]$. ■

Exemplo 2.30 Considere a asserção: $(\forall n \in \mathbb{Z})[n^2 - n + 11 \text{ é primo}]$.

Refutação. Considere n sendo instanciado com valor 11, ou seja, tem-se que $11^2 - 11 + 11 = 11^2$, agora desde que 11^2 é divisível por 11, tem-se que $11^2 - 11 + 11$ não é um número primo e, portanto, $n = 11$ é um contraexemplo que refuta a asserção, $(\forall n \in \mathbb{Z})[n^2 - n + 11 \text{ é primo}]$. ■

Exemplo 2.31 Considere a asserção: $(\forall A, B, C)[A - (B \cap C) = (A - B) \cap (A - C)]$.

Refutação. Assuma que $A = \{0, 1, 2, 3\}, B = \{0, 1\}$ e $C = \{1, 3\}$, logo tem-se que $A - (B \cap C) = \{0, 2, 3\}$, por outro lado, $(A - B) \cap (A - C) = \{2\}$, e claramente $\{0, 2, 3\} \neq \{2\}$, logo a instanciação $A = \{0, 1, 2, 3\}, B = \{0, 1\}$ e $C = \{1, 3\}$ que refuta a asserção, $(\forall A, B, C \text{ conjuntos})[A - (B \cap C) = (A - B) \cap (A - C)]$. ■

O leitor mais atento deve ter notado que refutar uma asserção universal, isto é, uma afirmação da forma $(\forall x \in X)[P(x)]$, nada mais é do que, apresentar exatamente uma instância de x que prova a asserção existencial $(\exists x \in X)[\neg P(x)]$ como verdadeira.

Agora o método para conseguir **refutar uma asserção existencial** consiste em mostrar que todos os x's no domínio do problema são tais que não satisfazem a propriedade (ou afirmação) exposta pela asserção, em outras palavras, deve-se fazer uma demostração de universalidade sobre a negação da asserção original, neste texto tal técnica será chamada de **refutação por totalidade**, a seguir são apresentados alguns exemplos de seu uso.

Exemplo 2.32 Considere a seguinte asserção sobre os números reais: $(\exists x \in \mathbb{R})[x^2 + 1 \leq x]$.

Refutação. Primeiramente note que a negação da asserção $(\exists x \in \mathbb{R})[x^2 + 1 \leq x]$ é exatamente a asserção $(\forall x \in \mathbb{R})[x^2 + 1 > x]$. Agora assuma que $x \in \mathbb{R}$, obviamente pelas propriedades da exponenciação sabe-se que $x^2 \geq x$, além disso, é claro que $x^2 + 1 > x^2$ e, portanto, $x^2 + 1 > x$, agora desde que x é um real qualquer pode-se concluir que a asserção $(\forall x \in \mathbb{R})[x^2 + 1 > x]$ é de fato verdadeira, consequentemente, sua negação é falsa, ou seja, a demonstração da universalidade de $(\forall x \in \mathbb{R})[x^2 + 1 > x]$ refuta qualquer possibilidade de que a asserção $(\exists x \in \mathbb{R})[x^2 + 1 \leq x]$ seja verdadeira. ∎

Exemplo 2.33 Considere a asserção sobre os números impares[a]: $(\exists x \in \overline{\mathbb{P}})[(\exists y \in \overline{\mathbb{P}})[x + y \notin \mathbb{P}]]$.

Refutação. Primeiramente note que a negação da asserção $(\exists x \in \overline{\mathbb{P}})[(\exists y \in \overline{\mathbb{P}})[x + y \notin \mathbb{P}]]$ é exatamente a asserção $(\forall x \in \overline{\mathbb{P}})[(\forall y \in \overline{\mathbb{P}})[x + y \in \mathbb{P}]]$. Agora assuma que $x \in \overline{\mathbb{P}}$ assim $x = 2i + 1$ com $i \in \mathbb{Z}$, além disso, suponha também que $y \in \overline{\mathbb{P}}$ logo $y = 2j + 1$ sendo $j \in \mathbb{Z}$, consequentemente, $x + y = 2(i + j + 1)$ fazendo $k = (i + j + 1)$ tem-se que $x + y = 2k$ e, portanto, $x + y \in \mathbb{P}$, logo a asserção $(\forall x \in \overline{\mathbb{P}})[(\forall y \in \overline{\mathbb{P}})[x + y \in \mathbb{P}]]$ é verdadeira e, dessa forma, sua demonstração refuta qualquer possibilidade da asserção $(\exists x \in \overline{\mathbb{P}})[(\exists y \in \overline{\mathbb{P}})[x + y \notin \mathbb{P}]]$ ser verdadeira. ∎

[a] O símbolo $\mathbb{P}$ denotada o conjunto dos números inteiros pares.

Por fim, a tarefa de refutar uma implicação (se α, então β), consiste em assumir o antecedente como sendo verdadeiro e mostrar a partir desta suposição que a negação do consequente β é verdadeira, em outras palavras, deve-se assumir α e deduzir $\neg\beta$, a seguir alguns exemplos são mostrados.

Exemplo 2.34 Considere a asserção: Se $x \in \mathbb{P}, y \notin \overline{\mathbb{P}}$, então $2x + 3j \in \mathbb{P}$.

Refutação. Suponha que $x \in \mathbb{P}$ e $y \notin \overline{\mathbb{P}}$, logo $x = 2i$ e $y = 2j + 1$, dessa forma tem-se que,

$$
\begin{aligned}
2x + 3y &= 4i + 6j + 3 \\
&= 2(2i + 3j + 1) + 1
\end{aligned}
$$

agora fazendo $k = 2i + 3j + 1$ tem-se que $2x + 3y = 2k + 1$ e, portanto, $2x + 3y \in \overline{\mathbb{P}}$, consequentemente, a asserção, "Se $x \in \mathbb{P}, y \notin \overline{\mathbb{P}}$, então $2x + 3j \in \mathbb{P}$" é falsa. ∎

Exemplo 2.35 Considere a asserção: Se $a, b \in \mathbb{N}$, então $a + a < 2ab$.

Refutação. Suponha que $a, b \in \mathbb{N}$, agora para um contra-exemplo note que 0 é uma instanciação válida de a nos moldes descrito pela asserção, além disso, pela instanciação $a = 0$ tem-se claramente que $a + a = 2ab$ independentemente do valor de b, e isto refuta a asserção "Se $a, b \in N$, então $a + a < 2ab$", mostrando que a mesma é falsa. ∎

Exemplo 2.36 Considere a asserção: Se $n \in \mathbb{N}$ e n é um quadrado perfeito, então $2n$ é divisível por 4.

Refutação. Suponha que $n \in \mathbb{N}$ e n é um quadrado perfeito, obviamente uma das instanciações para n é exatamente o número natural 9, note entretanto que $2 \cdot 9 = 18$ e 18 não é divisível por 4, assim a asserção "Se $n \in \mathbb{N}$ e n é um quadrado perfeito, então $2n$ é divisível por 4" é falsa. ∎

2.10 Questionário

Questão 2.1 Demonstre as seguintes asserções.

(a). Dado $a, b, \in \mathbb{R}$. Se $a < b < 0$, então $a^2 > b^2$.

(b). Dado $a, b, \in \mathbb{R}$. Se $0 < a < b$, então $\dfrac{1}{b} < \dfrac{1}{a}$.

(c). Dado $a \in \mathbb{R}$. Se $a^3 > a$, então $a^5 > a$.

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

(e). Sejam $a, b \in \mathbb{R}$. Se $a < b$, então $\dfrac{a + b}{2} < b$.

(f). Dado $x \in \mathbb{R}$ e $x \neq 0$. Se $\dfrac{\sqrt[3]{x} + 5}{x^2 + 6} = \dfrac{1}{x}$, então $x \neq 8$.

(g). Sendo $a, b, c, d \in \mathbb{R}$ com $0 < a < b$ e $d > 0$. Se $ac \geq bd$, então $c > d$.

(h). Dado $x, y \in \mathbb{R}$ e $3x + 2y \leq 5$. Se $x > 1$, então $y < 1$.

(i). Sejam $x, y \in \mathbb{R}$. Se $x^2 + y = -3$ e $2x - y = 2$, então $x = -1$.

(j). Se $n \in \mathbb{Z}$ e $n \in \{x \mid 4 \leq x \leq 12, x \text{ não é primo}\}$, então n é a soma de dois números primos.

(k). Dado $n \in \mathbb{N}$. Se $n \leq 3$, então $n! \leq 2^n$.

(l). Dado $n \in \mathbb{N}$. Se $2 \leq n \leq 4$, então $n^2 \geq 2^n$.

(m). Se n é um inteiro par, então $n^2 - 1$ é ímpar.

(n). Seja $n_0 \in \mathbb{N}$ e $n_1 = n_0 + 1$. Tem-se que $n_0 n_1$ é par.

(o). Se $n \in \mathbb{Z}$, então $n^2 + n$ é par.

(p). Se $n \in \mathbb{Z}$ e n é par, então n^2 é divisível por 4.

(q). Para todo $n \in \mathbb{Z}$ o número $3(n^2 + 2n + 3) - 2n^2$ é um quadrado perfeito.

(r). Dado $n \in \mathbb{Z}$. Se $x > 0$, então $x + 1 > 0$.

(s). Se n é ímpar, então n é a diferença de dois quadrados.

(t). Se $3n + 5 = 6k + 8$ com $k \in \mathbb{Z}$, então n é ímpar.

(u). Se n é par, então $3n + 2 = 6k + 2$ com $k \in \mathbb{Z}$.

(v). Se $x^2 + 2x - 3 = 0$, então $x \neq 2$.

(w). Dado $n, n_0, n_1 \in \mathbb{Z}$. Se n_0 e n_1 são ambos múltiplos de n, então $n_0 + n_1$ é também múltiplo n.

(x). Dado $x, y \in \mathbb{Z}$. Se xy não é múltiplo por n tal que $n \in \mathbb{Z}$, então $x + y$ é múltiplo de n.

(y). Dado $m, n, p \in \mathbb{Z}$. Se m é múltiplo de n e n é múltiplo de p, então m é múltiplo de p.

(z). Se x é ímpar, então $x^2 - x$ é par.

Questão 2.2 Prove que se A e $(B - C)$ são disjuntos, então $(A \cap B) \subseteq C$.
Questão 2.3 Prove que se $A \subseteq (B - C)$, então A e C são disjuntos.
Questão 2.4 Dado $x \in \mathbb{R}$ prove que:

(a). Se $x \neq 1$, então existe $y \in \mathbb{R}$ tal que $\dfrac{y+1}{y-2} = x$.

(b). Se existe um $y \in \mathbb{R}$ tal que $\dfrac{y+1}{y-2} = x$, então $x \neq 1$.

Questão 2.5 Considere que $\mathbb{P}$ e $\overline{\mathbb{P}}$ representam respectivamente o conjunto dos números inteiros pares e ímpares, assim demonstre as seguintes asserções.

(a). Para todo $x, y \in \overline{\mathbb{P}}$ tem-se que $x - y \in \mathbb{P}$.

(b). Para todo $x, y \in \mathbb{P}$ e todo $z \in \overline{\mathbb{P}}$ tem-se que $(x + y) + z \in \overline{\mathbb{P}}$.

(c). A soma de três elementos consecutivos de $\overline{\mathbb{P}}$ é um número múltiplo de 3.

Questão 2.6 Prove que $\sqrt{3} \notin \mathbb{Q}$.
Questão 2.7 Demonstre que: para todo $n \in \mathbb{Z}$, se $5n$ é ímpar, então n é ímpar.
Questão 2.8 Demonstre que $x^2 = 4y + 3$ não tem solução inteira.
Questão 2.9 Prove que todo número primo maior que 3 é igual a $6k + 1$ ou igual a $6k - 1$.
Questão 2.10 Considerando o conjunto dos números inteiros demonstre as seguintes asserções.

(a). Para todo x, y, z se x divide y e x divide z, então x divide $y + c$.

(b). Para todo x, y, z se xy divide yz e $z \neq 0$, então x divide y.

Questão 2.11 Considerando o conjunto $\mathbb{R}$ como universo do discurso demonstre as asserções a seguir:

(a). $(\forall x)[(\exists! y)[x^2 y = x - y]]$.

(b). $(\exists! x)[(\forall y)[xy + x - 4 = 4y]]$.

(c). $(\forall x)[x \neq 0 \land x \neq 1 \Rightarrow (\exists! y)[\frac{y}{x} = y - x]]$.

(d). $(\forall x)[x \neq 0 \Rightarrow (\exists! y)[(\forall z)[zy = \frac{z}{x}]]]$

Questão 2.12 Seja $\mathbb{U}$ um conjunto qualquer, demonstre as seguintes asserções:

(a). $(\exists! A \in \wp(U))[(\forall B \in \wp(U))[A \cup B = B]]$.

(b). $(\exists! A \in \wp(U))[(\forall B \in \wp(U))[A \cap B = B]]$.

Questão 2.13 Demonstre as condições suficientes e necessárias das asserções a seguir.

(a). Dado $x \in \mathbb{Z}$ tem-se que x é par se, e somente se, $3x + 5$ é impar.

(b). Dado $x \in \mathbb{Z}$ tem-se que x é impar se, e somente se, $3x + 9$ é par.

(c). Dado $x \in \mathbb{Z}$ tem-se que $x^3 + x^2 + x$ é par se, e somente se, x é par.

(d). Dado $x \in \mathbb{Z}$ tem-se que $x^2 + 4x + 5$ é impar se, e somente se, x é impar.

(e). Seja $x \in \mathbb{N}$ tem-se que x é impar se, e somente se, x^3 é impar.

(f). Sejam $x, y \in \mathbb{R}$ tem-se que $x^3 + x^2 y = y^2 + xy$ se, e somente se, $y = x^2$ ou $y = -x$.

(g). Sejam $x, y \in \mathbb{R}$ tem-se que $(x + y)^2 = x^2 + y^2$ se, e somente se, $x + y = x$ ou $x + y = y$.

(h). Dado $x \in \mathbb{Z}$ tem-se que x é múltiplo de 16 se, e somente se, x é múltiplo de $2, 4, 8$ e seu dobro é múltiplo de 32.

(i). Sejam $x, y \in \mathbb{Z}$ tem-se que $x = mdc(x, y)$ se, e somente se, $y = xn$ para algum $n \in \mathbb{Z}$.

(j). Sejam $x, y \in \mathbb{Z}$ tem-se que $y = mmc(x, y)$ se, e somente se, y é múltiplo de $x = yn$ para algum $n \in \mathbb{Z}$.

Questão 2.14 Para cada asserção a seguir apresente uma demonstração (no caso da asserção ser verdadeira) ou uma refutação (no caso da asserção ser falsa).

(a). Se $x, y \in \mathbb{R}$, então $|x + y| = |x| + |y|$.

(b). Existe $x \in \mathbb{R}$ tal que $|x| = |\sqrt{x}|$.

(c). Se $n \in \mathbb{Z}$ e $n^5 - n$ é par, então n é par.

(d). Para todo natural n, o inteiro da forma $2n^2 - 4n + 31$ é primo.

(e). Para todo natural n_1 e n_2 primos, o inteiro da forma $2n_1 + (n_2 - 1) + 1$ é impar.

(f). Não existe nenhum número inteiro n tal que $2n^2 - 1$ seja par.

(g). Se A e B são conjuntos quaisquer, então $\wp(A) - \wp(B) \subseteq \wp(A - B)$.

(h). Se A e B são conjuntos quaisquer e $A \cap B = \emptyset$, então $\wp(A) - \wp(B) \subseteq \wp(A - B)$.

(i). Se $x, y, z \in \mathbb{N}$ tal que xy, yz e xz tem a mesma paridade, então $x, y, z \in \mathbb{P}$ ou $x, y, z \in \overline{\mathbb{P}}$.

(j). Existe um conjunto $X \subseteq \mathbb{Z}$ tal que $X \cap \mathbb{N} \neq \emptyset$ mas $X \nsubseteq \mathbb{N}$.

(k). Existe um conjunto X tal que $\mathbb{R} \subseteq X$ e $\emptyset \in X$.

(l). Existem dois conjuntos X_1 e X_2 com $X_1 \neq X_2, X_1 \neq \emptyset$ e $X_2 \neq \emptyset$ tal que $\mathbb{Z}_+ \subseteq X_1 \cap X_2$ mas $\mathbb{Z} \nsubseteq X_1 \cup X_2$.

(m). Para todo $x, y \in \mathbb{Q}$ com $x < y$, existe um número irracional z para o qual $x < z < y$.

(n). Existe um natural n tal que $\sqrt{n+1} = p$ e p é primo.

(o). Existem dois números primos p_1 e p_2 tal que $p_1 + p_2 = 53$.

(p). Existem dois números primos p_1 e p_2 tal que $p_1 - p_2 = 1000$.

(q). Existem dois números primos p_1 e p_2 tal que $p_1 - p_2 = 97$.

(r). Existem dois números primos p_1 e p_2 tal que $p_1 < p_2$ e $2p_1 + p_2^2$ é impar.

(s). Dado $x, y \in \mathbb{R}$, se $x^3 < y^3$, então $x < y$.

(t). Para todo $x \in \mathbb{R}$ tem-se que $2^x \geq x + 1$.

(u). Existem $x, y \in \mathbb{Z}$ tal que $42x + 7y = 1$.

(v). Se existe $x \in \mathbb{N}$ para todo $y \in \mathbb{N}$ tal que $x - y \in \mathbb{Z}$ e $x - y \notin \mathbb{N}$, então $x = 0$.

Capítulo 3

Relações

> *"A matemática preocupa-se apenas com a enumeração e comparação de relações".*
>
> *Carl Friedrich Gauss*

3.1 Sobre Relações

A ideia de relação é um conceito frequentemente utilizado, seja no cotidiano das pessoas, seja na matemática [7]. Uma subárea da matemática de extrema importância para a Ciência da Computação, especificamente na área de banco de dados, é a álgebra relacional, que de forma resumida é o estudo das relações entre objetos de um mesmo espaço (conjunto).

Como comentado em [23], no cotidiano do mundo "real" existem diversos tipos de relacionamentos entre as entidades, por exemplo, imagine que duas pessoas, um homem jovem e um(a) garotinho(a) compartilham um ancestral comum, tal como um avô, assim pode-se dizer que os dois apresentam uma relação de parentesco, ou ainda que existe uma relação familiar entre os dois.

No que diz respeito ao universo matemático, a noção de relação entre os objetos é algo onipresente em todos os campos da matemática. Um exemplo clássico de relacionamento que se pode estabelecer entre dois números, x e y, é a ideia de dobro, isto é, x e y apresentam um relacionamento de dobro entre si no caso de $y = 2x$ ou $x = 2y$.

Note que de forma subliminar os exemplos anteriores caracterizam as relações de parentesco e dobro através da associação de elementos que juntos apresentavam uma certa propriedade, e nesse sentido uma relação nada mais é do que um conjunto definido sobre uma certa propriedade entre elementos de um espaço. A formalização das relações como sendo um conjunto será construída nas próximas seções.

3.2 Pares Ordenados e Produto Cartesiano

Da mesma forma que [1], neste documento será considerada a definição apresentada a seguir de par ordenado, sendo que tal definição foi apresentada pela primeira vez pelo grande matemático e lógico polonês Kazimierz Kuratowski (1896–1980).

Definição 3.1 — Par Ordenado. Sejam x e y elementos em um universo do discurso. O par ordenado entre x e y, denotado por (x, y), corresponde a seguinte igualdade:

$$(x, y) = \{x, \{x, y\}\}$$

Dado qualquer par ordenado (x, y) o elemento x é chamado de primeira componente do par ordenado, e o y é chamado de segunda componente do par ordenado. Além disso, como explicado em [46, 47], dois pares ordenados (x_1, y_1) e (x_2, y_2) serão ditos iguais[1] se, e somente se, $x_1 = x_2$ e $y_1 = y_2$.

Observação 3.1 — Igualdade perigosa! Não saia por aí dizendo que (x, y) é igual a $\{x, y\}$, ALiCIA vai te dar um grande sermão se você fizer isso! Pois note que, (x, y) consiste em um conjunto heterogêneo na forma $\{x, \{x, y\}\}$, enquanto, $\{x, y\}$ é um conjunto diferente, se não entendeu, ALiCIA recomenda que você volte ao Capítulo 1 e reveja a Definição 1.6, que descreve extamente a igualdade entre conjuntos!

De posse do conceito de par ordenado é possível definir uma nova operação entre conjuntos, tal operação recebe o nome de produto Cartesiano[2] e será de vital importância para em seguida apresentar as ideias ligadas ao conceito de relações.

Definição 3.2 — Produto Cartesiano. Sejam A e B dois conjuntos quaisquer, o produto Cartesiano entre A e B, denotado por $A \times B$, corresponde ao conjunto de todos os pares ordenados em que a primeira componente é um elemento de A e a segunda componente é um elemento de B, ou seja, tem-se que:

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

Exemplo 3.1 Dado os seguintes dois conjuntos $\{a, b, c\}$ e $\{-1, 1\}$ tem-se os seguintes produtos Cartesianos.

(a) $\{a, b, c\} \times \{-1, 1\} = \{(a, 1), (a, -1), (b, -1), (b, 1), (c, -1), (c, 1)\}$.

(b) $\{-1, 1\} \times \{a, b, c\} = \{(1, a), (1, b), (1, c), (-1, a), (-1, c), (-1, b)\}$.

[1] Este resultado segue direto da Definição 1.6, a prova deste fato ficará como exercício ao leitor.

[2] O nome produto Cartesiano provém do matemática francês René Descartes (1596–1650), que foi o primeiro a estudar tal operação conjuntista [46].

(c) $\{a, b, c\} \times \{a, b\} = \{(a, a), (a, b), (c, b), (b, a), (b, b), (c, a)\}$.

(d) $\{-1, 1\} \times \{1, -1\} = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$

Uma classe de casos particulares da aplicação do produto Cartesiano e a classe dos Cartesianos chamados de quadrados, no que se segue este documento apresenta formalmente a seguir o conceito de Cartesiano quadrado.

Definição 3.3 — Cartesiano quadrado. Seja A um conjunto qualquer. O produto Cartesiano quadrado de A, denotado por A^2, corresponde ao produto Cartesiano de A consigo mesmo, ou seja, tem-se que:

$$A^2 = \{(x, y) \mid x, y \in A\}$$

Tomando Notas 3.1 – Açúcar sintático! É bom ter em mente que A^2 é apenas uma forma simplificada ou doce (um açúcar sintático[a]) para escrever $A \times A$.

[a] O conceito de açúcar sintático (em inglês *syntactic sugar*), é uma expressão criada em 1964 por Peter J. Landin (1930–2009) em seus seminais trabalhos [36, 37, 38]. De forma direta um açúcar sintático diz respeito a uma sintaxe dentro da linguagem formal que tem por finalidade tornar suas construções mais fáceis de serem lidas e expressas, ou seja, um açúcar sintático é uma ferramenta para tornar o uso da linguagem mais doce (ou amigável) para o uso dos seres humanos.

Exemplo 3.2 Os itens (c) e (d) do Exemplo 3.1 são produtos Cartesianos quadrados.

Teorema 3.1 — Produto Cartesiano - absorção. Dado dois conjuntos A e B tem-se que, $A \times B = \emptyset$ se, e somente se, $A = \emptyset$ ou $B = \emptyset$.

Demonstração. $(\Rightarrow)$ Por contrapositiva assuma que $A \neq \emptyset$ e $B \neq \emptyset$, assim tem-se que existem $x \in A$ e $y \in B$, consequentemente, pela definição de produto cartesiano existe $(x, y) \in A \times B$, assim tem-se que, $A \times B \neq \emptyset$, e portanto, a afirmação: Se $A \times B = \emptyset$, então $A = \emptyset$ ou $B = \emptyset$ é verdadeira.

$(\Leftarrow)$ Suponha que $A = \emptyset$ ou $B = \emptyset$, assim tem-se claramente por vacuidade que $A \times B = \emptyset$. □

Teorema 3.2 — Produto Cartesiano - igualdade. Dado dois conjuntos A e B tem-se que, $A \times B = B \times A$ se, e somente se, $A = \emptyset$ ou $B = \emptyset$ ou $A = B$.

Demonstração. A prova desta asserção ficará como exercício ao leitor. □

O produto Cartesiano enquanto operação tem a propriedade de preservar a relação de inclusão à direta e à esquerda como pode ser visto a seguir.

Teorema 3.3 — Produto Cartesiano - monotonicidade à direita. Dado três conjuntos A, B e C tem-se que, $A \subset B$ se, e somente se, $A \times C \subset B \times C$.

Demonstração. ($\Rightarrow$) Suponha que $A \subset B$, logo por definição tem-se que todo $x \in A$ é tal que $x \in B$, e assim é óbvio que para todo $(x, y) \in A \times C$ tem-se que $(x, y) \in B \times C$, e portanto, pela definição de subconjunto tem-se que $A \times C \subseteq B \times C$, mas por hipótese tem-se que existe $x' \in B$ tal que $x' \notin A$, logo existe $(x', y) \in B \times C$ tal que $(x', y) \notin A \times C$, consequentemente, $A \times C \subset B \times C$.

($\Leftarrow$) Assuma que $A \times C \subset B \times C$, logo tem-se que para todo $(x, y) \in A \times C$ tem-se que $(x, y) \in B \times C$, mas note que por definição $(x, y) \in A \times C$ se, e somente se, $x \in A$ e de forma similar tem-se que $(x, y) \in B \times C$ se, e somente se, $x \in B$, dessa forma tem-se que $A \subset B$, além disso, por hipótese existe um $(x', y) \in B \times C$ tal que $(x', y) \notin A \times C$, portanto, é claro que existe $x' \in B$ tal que $x' \notin A$, consequentemente, $A \subset B$. □

Teorema 3.4 — Produto Cartesiano - monotonicidade à esquerda. Dado três conjuntos A, B e C tem-se que, $A \subset B$ se, e somente se, $C \times A \subset C \times B$.

Demonstração. Similar a demonstração do Teorema 3.3. □

O próximo resultado mostra que a operação de produto Cartesiano se distribui sobre as operações de união, interseção e diferença.

Teorema 3.5 — Leis de Distributividade do Cartesiano. Dado três conjuntos A, B e C tem-se que:

(i) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

(ii) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

(iii) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(iv) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

(v) $A \times (B - C) = (A \times B) - (A \times C)$.

(vi) $(A - B) \times C = (A \times C) - (B \times C)$.

(vii) $A \times (B \ominus C) = (A \times B) \ominus (A \times C)$.

(vii) $(A \ominus B) \times C = (A \times C) \ominus (B \times C)$.

Demonstração. Sejam A, B e C conjuntos tem-se que:

(i)

$$\begin{aligned}
A \times (B \cap C) &= \{(x, y) \mid x \in A, y \in (B \cap C)\} \\
&= \{(x, y) \mid x \in (A \cap A), y \in (B \cap C)\} \\
&= \{(x, y) \mid x \in A, x \in A, y \in B, y \in C\} \\
&= \{(x, y) \mid x \in A, y \in B, x \in A, y \in C\} \\
&= \{(x, y) \mid x \in A, y \in B\} \cap \{(x, y) \mid x \in A, y \in C\} \\
&= (A \times B) \cap (A \times C)
\end{aligned}$$

(ii) Similar ao item anterior.

(iii)

$$\begin{aligned}
A \times (B \cup C) &= \{(x, y) \mid x \in A, y \in (B \cup C)\} \\
&= \{(x, y) \mid x \in (A \cup A), y \in (B \cup C)\} \\
&= \{(x, y) \mid x \in A \text{ ou } x \in A, y \in B \text{ ou } y \in C\} \\
&= \{(x, y) \mid x \in A, y \in B \text{ ou } x \in A, y \in C\} \\
&= \{(x, y) \mid x \in A, y \in B\} \cup \{(x, y) \mid x \in A, y \in C\} \\
&= (A \times B) \cup (A \times C)
\end{aligned}$$

(iv) Similar ao item anterior.

(v)

$$\begin{aligned}
A \times (B - C) &= \{(x, y) \mid x \in A, y \in (B - C)\} \\
&= \{(x, y) \mid x \in A \cap A, y \in (B - C)\} \\
&= \{(x, y) \mid x \in A, x \in A, y \in B, y \notin C\} \\
&= \{(x, y) \mid (x, y) \in A \times B, (x, y) \notin (A \times C)\} \\
&= (A \times B) - (A \times C)
\end{aligned}$$

(vi) Similar ao item anterior.

(vii)

$$\begin{aligned}
A \times (B \ominus C) &\overset{Cor.\ 1.1}{=} A \times ((B \cup C) - (B \cap C)) \\
&\overset{Teo.\ 3.5\text{(v)}}{=} (A \times (B \cup C)) - (A \times (B \cap C)) \\
&\overset{Teo.\ 3.5\text{(iii)}}{=} ((A \times B) \cup (A \times C)) - (A \times (B \cap C)) \\
&\overset{Teo.\ 3.5\text{(i)}}{=} ((A \times B) \cup (A \times C)) - ((A \times B) \cap (A \times C)) \\
&\overset{Cor.\ 1.1}{=} (A \times B) \ominus (A \times C)
\end{aligned}$$

(viii) Similar ao item anterior.

□

O conceito do produto Cartesiano pode, como explicado em [46, 47], ser estendido a poder operar com mais de dois conjuntos, sendo essa extensão realizada de forma natural apenas aumentando um número de componentes nos elementos do conjunto resultante ao conjunto do produto, ou seja, os elementos deixam de ser simples pares ordenados para serem tuplas ordenadas. A seguir este conceito é formalizado.

Definição 3.4 — Produto Cartesiano n-ário. Dado $n \geq 2$ e sejam $A_1, A_2, \cdots, A_n$ conjuntos quaisquer, o produto Cartesiano n-ário, denotado por $A_1 \times \cdots \times A_n$, corresponde ao conjunto formado por todas as tuplas da forma $(a_1, \cdots, a_n)$ tal que para todo $1 \leq i \leq n$ tem-se que $a_i \in A_i$.

Em um produto Cartesiano n-ário da forma $A_1 \times \cdots \times A_n$ cada A_i com $1 \leq i \leq n$ é chamado de i-ésimo fator do produto. Outra forma comum de denotar o produto Cartesiano n-ário muito encontrada na literatura é usando o símbolo do produtório, ou seja, $\prod_{i=1}^{n} A_i$, ou ainda na forma açucarada, A^n.

Exemplo 3.3 Dado os conjuntos $\{-1, 1\}, \{a, b\}$ e $\{0, 1\}$ tem-se os seguintes produtos Cartesianos n-ários:

$$\begin{aligned}
\{-1,1\} \times \{a,b\} \times \{0,1\} &= \{(-1,a,0),(-1,a,1),(-1,b,0),(-1,b,1),\\
&\quad (1,a,0),(1,a,1),(1,b,0),(1,b,1)\}
\end{aligned}$$

$$\begin{aligned}
\{-1,1\} \times \{-1,1\} \times \{a,b\} \times \{a,b\} &= \{(-1,1,a,a),(-1,1,a,b),\\
&\quad (-1,1,b,a),(-1,1,b,b),\\
&\quad (-1,-1,a,a),(-1,-1,a,b),\\
&\quad (-1,-1,b,a),(-1,-1,b,b),\\
&\quad (1,-1,a,a),(1,-1,a,b),\\
&\quad (1,-1,b,a),(1,-1,b,b),\\
&\quad (1,1,a,a),(1,1,a,b),\\
&\quad (1,1,b,a),(1,1,b,b)\}
\end{aligned}$$

Exemplo 3.4 Dado o conjunto $\{0, 1\}$ tem-se que

$$\begin{aligned}
\{0,1\}^5 &= \{(0,0,0,0,0),(0,0,0,0,1),(0,0,0,1,0),(0,0,0,1,1),(0,0,1,0,0),\\
&\quad (0,0,1,0,1),(0,0,1,1,0),(0,0,1,1,1),(0,1,0,0,0),(0,1,0,0,1),\\
&\quad (0,1,0,1,0),(0,1,0,1,1),(0,1,1,0,0),(0,1,1,0,1),(0,1,1,1,0),\\
&\quad (1,0,0,0,0),(1,0,0,0,1),(1,0,0,1,0),(1,0,0,1,1),(1,0,1,0,0),\\
&\quad (1,0,1,1,0),(1,0,1,1,1),(1,1,0,0,0),(1,1,0,0,1),(1,1,0,1,0),\\
&\quad (1,1,1,0,0),(1,1,1,0,1),(1,1,1,1,0),(1,1,1,1,1),(0,1,1,1,1),\\
&\quad (1,0,1,0,1),(1,1,0,1,1)\}
\end{aligned}$$

Exemplo 3.5 São produtos Cartesianos n-ários:

(a) $\{a, b, c\}^2 = \{(a, a), (c, b), (a, c), (a, b), (c, c,)(b, a), (b, b), (b, c), (c, a)\}$.

(b) $\{0, 1\}^2 = \{(1, 0), (1, 1), (0, 1), (0, 0)\}$.

(c) $\{1\}^9 = \{(1, 1, 1, 1, 1, 1, 1, 1, 1)\}$.

(d) $\{a, (1, 2)\}^2 = \{(a, a), (a, (1, 2)), ((1, 2), a), ((1, 2), (1, 2))\}$.

(e) $\{a, b\} \times \{0\}^2 = \{(a, (0, 0)), (b, (0, 0))\}$.

(f) $\{1\}^2 \times \{1\} = \{((1, 1), 1)\}$.

Quando os conjuntos $A_1, A_2, \cdots, A_n$ são todos conjuntos finitos, uma estratégia muito utilizada para se obter e também representar o mecanismo de construção das tuplas $(a_1, a_2, \cdots, a_n)$ pertencentes ao produto Cartesiano n-ário $A_1 \times A_2 \times \cdots \times A_n$ é usando a noção de diagrama de árvore [46, 47].

Tomando Notas 3.2 – Cuidado ao desenhar árvores cartesianas! De forma contrária ao que acontecer nos diagramas de árvores nas área de estrutura de dados [69], linguagens formais [8, 34, 43] e compiladores [3, 16], os diagramas de árvore na teoria dos conjuntos são construídos de forma horizontal no sentido da esquerda para à direita.

Em um diagrama de árvore o número de níveis na árvore é igual ao número de conjuntos envolvidos no Cartesiano mais 2, ou seja, para cada produto Cartesiano n-ário, o número de níveis na árvore que gera/representa tal cartesiano é igual a $n + 2$.

Dado então os conjuntos no Cartesiano $A_1 \times \cdots \times A_n$, o diagrama é construindo por níveis da seguinte forma:

1. O nível inicial da árvore (nível 0) é colocado o símbolo de inicio da árvore (neste documento será usado o $*$ como símbolo inicial).

2. Para todo $1 \leq i \leq n$, cada nível i do diagrama vai ser preenchido pelos elementos do conjunto A_i[3].

3. Por fim, no último nível da árvore (ou nível EPC) estão os elementos do produto Cartesiano em si.

Exemplo 3.6 Dado os conjuntos $\{-1, 1\}, \{a, b\}$ e $\{-1, 1\}$ tem-se que o produto Cartesiano $\{-1, 1\} \times \{a, b\} \times \{-1, 1\}$ pode ser representado pelo diagrama esboçado na Figura 3.1.

[3]Como cada A_i é finito, cada $x \in A_i$ será repetido exatamente 2^{i-1} no nível i.

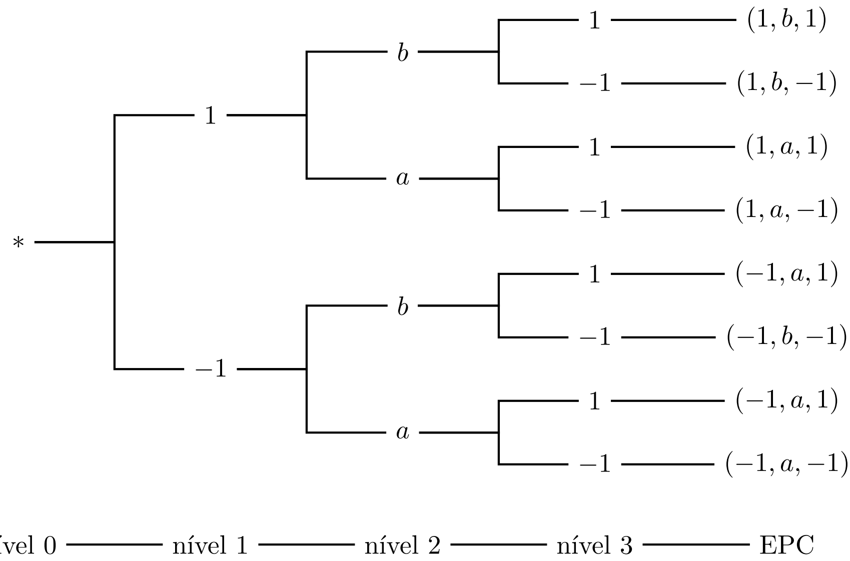


Figura 3.1: Diagrama de árvore para o Cartesiano $\{-1, 1\} \times \{a, b\} \times \{1, -1\}$.

Apesar de ser uma ótima forma prática de representar e visualizar o produto Cartesiano, os diagramas de árvores tendem a não ser adotados com frequência pois seu crescimento se dá em proporções fatoriais, o que torna sua construção facilmente complexa.

Observação 3.2 ALiCIA quer que você fique sempre atento a alguns fatos de cunho sintático a respeito do produto Cartesiano, ela chama sua atenção para o Exemplo 3.5, em tal exemplo é mostrado de forma explicita que $A \times B \times C \neq A \times (B \times C) \neq (A \times B) \times C$[a].

[a] No primeiro produto os elementos gerados são da forma (x, y, z), já no segundo os elementos terão a forma $(x, (y, z))$, e por fim, no terceiro produto os elementos tem a seguinte forma $((x, y), z)$ sendo $x \in A, y \in B$ e $z \in C$. Além disso, tem-se que o produto Cartesiano $A^n \times B = (\underbrace{A \times \cdots \times A}_{n-\text{vezes}}) \times B$.

3.3 Relações

Da mesma forma que foi apresentado em [1], este documento irá nesta seção tratar do conceito de relações binária e suas propriedades. O conceito de relações n-ária muito importante na matemática e na teoria de banco de dados não será estudado neste documento.

Definição 3.5 — Relação binária. Seja A e B dois conjuntos, uma relação R de A em B é qualquer subconjunto de $A \times B$, isto é, $R \subseteq (A \times B)$.

Tomando Notas 3.3 – Açúcar sintático. Dado R uma relação binária de A em B a sintaxe da teoria dos conjuntos e de pares ordenados permite que seja escrito que $(x, y) \in R$, entretanto, está escrita é geralmente substituída por $x \ R \ y$. E no caso de $(x, y) \notin R$ é escrito simplesmente $x \not R \ y$.

A semântica das palavras $x \ R \ y$ e $x \not R \ y$ podem ser interpretadas respectivamente como: "x está R-relacionado (está relacionado por R) com y" e "x não está R-relacionado (não está relacionado por R) com y". Em algumas obras como [14], é possível ver a sintaxe $x \underset{\rightarrow}{R} y$ para designar que $(x, y) \in R$, neste documento o autor irá optar sempre que possível pelo açúcar sintática descrito na Nota 3.3, e quando não for possível (ou conveniente) será usado a sintaxe padrão da teoria dos conjuntos e dos pares ordenados.

Definição 3.6 — Domínio e Imagem. Seja R uma relação de A em B, o domínio de R, denotado por $Dom(R)$, corresponde ao conjunto de todos os elementos de A que são a primeira coordenada de $x \ R \ y$, ou seja,

$$Dom(R) = \{x \in A \mid x \ R \ y\}$$

e a imagem de R, denotada por $Ima(R)$, corresponde ao conjunto de todos os elementos de B que são a segunda coordenada de $x \ R \ y$, ou seja,

$$Ima(R) = \{y \in B \mid x \ R \ y\}$$

Exemplo 3.7 Seja $R = \{(a, 1), (b, -1), (c, 1), (b, 1), (c, -1)\}$ uma relação tem-se que $Dom(R) = \{a, b, c\}$ e $Ima(R) = \{1, -1\}$.

Exemplo 3.8 Dado a relação $Q = \{(x, y) \in \mathbb{N}^2 \mid x^2 = y\}$ tem-se que $Dom(Q) = \{x \in \mathbb{N} \mid (\exists y \in \mathbb{N})[\sqrt{y} = x]\}$ e $Ima(Q) = \{y \in \mathbb{N} \mid (\exists x \in \mathbb{N})[x^2 = y]\}$

Exemplo 3.9 Uma relação binária R famosa é aquela usada para representar o conjunto das frações positivas, tal relação é definida como $F = \{(x, y) \mid x \in \mathbb{N}, y \in (\mathbb{N} - \{0\})\}$, note que a fração $\dfrac{1}{12}$ por exemplo corresponde ao elemento $1 \ F \ 12$.

Dada qualquer relação R sempre é possível obter uma nova relação a partir de

R, essa nova relação recebe o nome de relação inversa ou oposta.

Definição 3.7 — Relação inversa. Seja R uma relação. A relação inversa (ou oposta) de R, denotada por R^{-1}, corresponde ao seguinte conjunto:

$$R^{-1} = \{(y, x) \mid x \; R \; y\}$$

Exemplo 3.10 Considere a relação R do Exemplo 3.7, tem-se que a relação inversa de R corresponde ao conjunto $R^{-1} = \{(1, a), (-1, b), (1, c), (-1, c), (1, b)\}$.

Exemplo 3.11 Dado a relação $P = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a = b^2\}$ tem-se a inversa de P é exatamente a relação $R = \{(b, a) \in \mathbb{N} \times \mathbb{N} \mid b = \sqrt{a}\}$, isto é, $R = P^{-1}$.

Um fato básico para qualquer relação R é que $(R^{-1})^{-1} = R$. Em outras palavras, tal igualdade descreve que a reversa de uma relação, vista como uma operação é sempre involutiva, assim como a negação e o complemento.

Proposição 3.1 Se $R \subseteq A \times B$, então $R^{-1} \subseteq B \times A$.

Demonstração. Suponha que $R \subseteq A \times B$, logo todo $(x, y) \in A$ é tal que $(y, x) \in R^{-1}$, mas de $R \subseteq A \times B$ tem-se que $(x, y) \in A \times B$, consequentemente, por definição $x \in A$ e $y \in B$ e, portanto, $(y, x) \in B \times A$, consequentemente, $R^{-1} \subseteq B \times A$. □

O leitor atento pode notar que o resultado da Proposição 3.1 pode ser estendido para relacionar diretamente duas relações, e isso é feito como se segue.

Teorema 3.6 Se R e S são relações tais que $R \subseteq S$, então $R^{-1} \subseteq S^{-1}$.

Demonstração. Similar ao raciocínio da demonstração da Proposição 3.1. □

Uma vez que relações são conjuntos pode-se falar sobre as operações sobre relações, aqui não serão tratadas as operações triviais de união, interseção, complemento e diferença. Para essas operações é recomendável que o leitor retorne para revisar o texto apresentado na Seção 1.3 que trata exatamente de tais operações.

Uma operação natural que surge para as relações é a noção de composição entre duas relações R_1 e R_2, a ideia da composição é gerar uma terceira relação a partir das relações iniciais. A seguir este documento apresenta formalmente o conceito de composição.

Definição 3.8 — Composição de relações. Seja R_1 uma relação de A em B e seja R_2 uma relação de B em C, a composição de R_1 e R_2, denotada por $R_1 \bullet R_2$, corresponde ao seguinte conjunto:

$$R_1 \bullet R_2 = \{(x, z) \mid (\exists y \in B)[x \; R_1 \; y \text{ e } y \; R_2 \; z]\}$$

Proposição 3.2 Seja R_1 uma relação de A em B e seja R_2 uma relação de B em C, então tem-se que:

(i) $Dom(R_1 \bullet R_2) \subseteq Dom(R_1)$.

(ii) $Ima(R_1 \bullet R_2) \subseteq Ima(R_2)$.

Demonstração. Trivial pela própria Definição 3.8. $\square$

Exemplo 3.12 Sejam $R = A \times B$ e $Q = B \times C$ tem-se que $R \bullet Q = A \times C$.

Exemplo 3.13 Dado a relação $R_1 = \{(a, b), (i, b), (o, c), (o, e)\}$ e outra relação $R_2 = \{(b, 1), (b, -1), (c, 3), (d, 4)\}$ tem-se então que a composição de R_1 e R_2 é exatamente igual a relação $R = \{(a, 1), (a, -1), (i, 1), (i, -1), (o, 3)\}$.

Teorema 3.7 — Monotonicidade da Composição de Relações. Seja R_1 e R_2 relações de A em B. Se $R_1 \subseteq R_2$, então para toda relação R_3 de B em C tem-se que $(R_1 \bullet R_3) \subseteq (R_2 \bullet R_3)$.

Demonstração. Suponha que R_1 e R_2 são ambas relações de A em B e que $R_1 \subseteq R_2$, agora note que para qualquer relação R_3 de B em C tem-se por definição que $(x, z) \in (R_1 \bullet R_3)$ se, e somente se, $(\exists y \in B)[x\ R_1\ y$ e $y\ R_3\ z]$, mas uma vez que, $R_1 \subseteq R_2$ é claro que $(\exists y \in B)[x\ R_2\ y$ e $y\ R_3\ z]$, e assim $(x, z) \in (R_2 \bullet R_3)$, portanto, $(R_1 \bullet R_3) \subseteq (R_2 \bullet R_3)$, concluindo assim a prova. $\square$

Corolário 3.1 Se R_1, R_2, S_1, S_2 são relações tais que $R_1 \subseteq R_2$ e $S_1 \subseteq S_2$, então $(R_1 \bullet S_1) \subseteq (R_2 \bullet S_2)$.

Demonstração. Suponha que R_1, R_2, S_1, S_2 são relações tais que $R_1 \subseteq R_2$ e $S_1 \subseteq S_2$, assim pelo Teorema 3.7 tem-se que $(R_1 \bullet S_1) \subseteq (R_2 \bullet S_1)$. Agora note que por definição $(x, z) \in (R_2 \bullet S_1)$ se, e somente se, $(\exists y \in Dom(S_1))[x\ R_2\ y$ e $y\ S_1\ z]$, mas uma vez que $S_1 \subseteq S_2$ tem-se que $Dom(S_1) \subseteq Dom(S_2)$ e $Ima(S_1) \subseteq Ima(S_2)$ e assim é claro que $(\exists y \in Dom(S_2))[x\ R_2\ y$ e $y\ S_2\ z]$, logo $(x, z) \in (R_2 \bullet S_2)$, consequentemente pela definição de subconjunto tem-se que $(R_2 \bullet S_1) \subseteq (R_2 \bullet S_2)$. E portanto, $(R_1 \bullet S_1) \subseteq (R_2 \bullet S_2)$. $\square$

Tomando Notas 3.4 – Um novo símbolo! Nas próximas demonstrações aparece o símbolo da equivalência (semântica) lógica $\Longleftrightarrow$, o mesmo pode ser interpretado pela sentança, “se, e somente, se”.

Os próximos resultados estabelecem propriedades algébricas importantes para a operação de composição de relações.

Teorema 3.8 Seja R_1 uma relação de A em B e seja R_2 uma relação de B em C tem-se que $(R_1 \bullet R_2)^{-1} = R_2^{-1} \bullet R_1^{-1}$.

Demonstração. Dado R_1 uma relação de A em B e seja R_2 uma relação de B em C logo,

$$\begin{aligned}
(x,z) \in (R_1 \bullet R_2)^{-1} &\iff (z,x) \in (R_1 \bullet R_2) \\
&\overset{Def.3.8}{\iff} (\exists y \in B)[(z,y) \in R_1 \text{ e } (y,x) \in R_2] \\
&\iff (\exists y \in B)[(y,z) \in R_1^{-1} \text{ e } (x,y) \in R_2^{-1}] \\
&\iff (\exists y \in B)[(x,y) \in R_2^{-1} \text{ e } (y,z) \in R_1^{-1}] \\
&\iff (x,z) \in R_2^{-1} \bullet R_1^{-1}
\end{aligned}$$

e assim pela Definição 1.6 tem-se que $(R_1 \bullet R_2)^{-1} = R_2^{-1} \bullet R_1^{-1}$ o que completa a prova. □

Teorema 3.9 Seja R_1 uma relação de A em B e seja R_2 uma relação de B em C e R_3 uma relação de C em D tem-se que $(R_1 \bullet R_2) \bullet R_3 = R_1 \bullet (R_2 \bullet R_3)$.

Demonstração. Dado três relações R_1 de A em B, R_2 de B em C e R_3 de C em D tem-se por definição que, $(x,z) \in (R_1 \bullet R_2) \bullet R_3$ se, e somente se, existe $w \in C$ tal que $(x,w) \in (R_1 \bullet R_2)$ e $(w,z) \in R_3$, mas isso só é possível se, e somente se, $\exists y \in B$ tal que $(x,y) \in R_1$ e $(y,w) \in R_2$. Mas assim pela Definição 3.8 tem-se que $(y,z) \in R_2 \bullet R_3$, o que irá implicar que $(x,z) \in R_1 \bullet (R_2 \bullet R_3)$ e, portanto, tem-se que $(x,z) \in (R_1 \bullet R_2) \bullet R_3 \iff (x,z) \in R_1 \bullet (R_2 \bullet R_3)$, logo pela Definição 1.6 tem-se que $(R_1 \bullet R_2) \bullet R_3 = R_1 \bullet (R_2 \bullet R_3)$. □

Teorema 3.10 Dado duas relações R_1 e R_2 e A, B e C conjuntos. Se $R_1 \subset A \times B$ e $R_2 \subset B \times C$, então $R_1 \bullet R_2 \subset A \times C$.

Demonstração. Suponha que $R_1 \subset A \times B$ e $R_2 \subset B \times C$ logo tem-se que se $(x,y) \in R_1 \bullet R_2$ logo por definição existe $z \in B$ tal que $(x,z) \in R_1$ e $(z,y) \in R_2$, mas assim é claro que $(x,z) \in A \times B$ e $(z,y) \in B \times C$ e, portanto, $(x,y) \in A \times C$. Consequentemente, $R_1 \bullet R_2 \subset A \times C$. □

Teorema 3.11 Seja A, B e C conjuntos. Então tem-se que:

(1) Se $A \cap B \neq \emptyset$, então $(A \times B) \bullet (A \times B) = A \times B$.

(2) Se $A \cap B = \emptyset$, então $(A \times B) \bullet (A \times B) = \emptyset$.

(3) Se $B \neq \emptyset$, então $(B \times C) \bullet (A \times B) = A \times C$.

Demonstração. Aqui será demonstrado só o fato (1) ficando o (2) e (3) como exercício ao leitor. Dado A, B e C conjuntos, assuma que $A \cap B \neq \emptyset$, agora note que para todo $(x,y) \in (A \times B) \bullet (A \times B)$ tem-se que pelo fato de A e B não serem disjuntos sempre existe um $\exists z \in A \cap B$ tal que $(x, z) \in (A \times B)$ e $(z, y) \in (A \times B)$, portanto, $(x, y) \in A \times B$, logo pela Definição 1.6 tem-se que $(A \times B) \bullet (A \times B) = A \times B$. $\square$

Teorema 3.12 Dado duas relações R_1 e R_2 tem-se que:

(1) $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$.

(2) $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$.

Demonstração. Sejam R_1 e R_2 duas relações logo,

(1) Tem-se trivialmente que,

$$\begin{aligned}
(x, y) \in (R_1 \cup R_2)^{-1} &\iff (y, x) \in (R_1 \cup R_2) \\
&\iff (y, x) \in R_1 \text{ ou } (y, x) \in R_2 \\
&\iff (x, y) \in R_1^{-1} \text{ ou } (x, y) \in R_2^{-1} \\
&\iff (x, y) \in R_1^{-1} \cup R_2^{-1}
\end{aligned}$$

logo pela Definição 1.6 tem-se que $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$.

(2) A demonstração é similar ao item anterior.

$\square$

3.4 Tipos ou Propriedades das Relações Binárias

Deste ponto em diante todas as relações consideradas até o final deste capítulo serão relações binárias sobre um conjunto não vazio A genérico, ou seja, tem-se que se R for uma relação, então $R \subseteq A \times A$. Dito isto, agora serão apresentados os "tipos", ou na visão de [1], as propriedades que as relações binárias sobre um conjunto podem ser possuir.

Definição 3.9 — Tipo Identidade. Uma relação R é dita ser uma relação de identidade (ou relação idêntica [1]) sempre que R é igual ao conjunto $\{(x, x) \mid x \in A\}$.

Exemplo 3.14 Seja $A = \{1, 2, 3, 4\}$ a relação $M = \{(3, 3), (1, 1), (2, 2), (4, 4)\}$ é uma relação de identidade, já a relação $Q = \{(1, 1), (2, 2), (3, 4)\}$ não é uma relações de identidade.

Exemplo 3.15 Dado o conjunto $\mathbb{N}$, a relação $R = \{(x, y) \in \mathbb{N}^2 \mid x - y = 0\}$ é uma relação de identidade, já a relação $S = \{(x, y) \in \mathbb{N}^2 \mid x - y > 0\}$ não é uma relação de identidade pois $(5, 4) \in S$.

Tomando Notas 3.5 – Um nome especial! Dado que a relação de identidade possui exatamente todos os pares da forma (x, x), é comum chamar esta relação de identidade do conjunto A, ou simplesmente identidade de A, que costuma também ser denotado por Id_A.

Teorema 3.13 — Neutralidade da relação de identidade. Se R é uma relação sobre A, então as seguintes igualdade são verdadeiras:

(i) $R \bullet Id_A = R$.

(ii) $Id_A \bullet R = R$.

Demonstração. (i) Suponha que R é uma relação sobre A, assim tem-se que:

$$\begin{aligned} (x, y) \in R \bullet Id_A &\iff (\exists y \in A)[x \; R \; y \text{ e } y \; Id_A \; y] \\ &\iff (x, y) \in R \end{aligned}$$

Portanto, $R \bullet Id_A = R$. (ii) Similar a demonstração do item anterior. □

Proposição 3.3 Se A é um conjunto não vazio, então $Id_A^{-1} = Id_A$.

Demonstração. Trivial pelas Definições 3.7 e 3.9. □

Definição 3.10 — Tipo Reflexivo. Uma relação R é dita ser reflexiva quando para todo $x \in A$ tem-se que $x \; R \; x$.

Um leitor atento pode perceber que a relação identidade de um conjunto é sempre reflexiva, porém, o oposto não é verdadeiro como exposto no exemplo a seguir.

Exemplo 3.16 Dado o conjunto $A = \{a, b, c\}$ tem-se que:

(a) $K = \{(a, a), (b, c), (b, b), (c, c), (a, c), (c, a)\}$ é uma relação reflexiva, mas não é a identidade do conjunto A.

(a) $M = \{(a, a), (b, b), (c, c)\}$ é uma relação reflexiva e é também a relação identidade do conjunto A.

Como dito em [1], uma relação R não será reflexiva quando existir pelo menos um $x \in A$ tal que $x \not{R} \; x$.

Exemplo 3.17 Dado o conjunto $L = \{0, 0.5, 1\}$ tem-se que o conjunto Q formado pelos elementos $(0, 0), (0, 0.5)$ e $(1, 1)$ não é uma relação reflexiva, pois $0.5 \not{R} \; 0.5$, ou seja, $(0.5, 0.5) \notin Q$.

O próximo resultado estabelece uma caracterização para as relações serem reflexivas, isto é, tal resultado apresenta as condições suficientes e necessárias para que uma relação seja reflexiva.

Teorema 3.14 — Caracterização das Relações Reflexivas. Uma relação R é reflexiva se, e somente se, $Id_A \subset R$.

Demonstração. ($\Rightarrow$) Suponha que R seja reflexiva, logo por definição para todo $x \in A$ tem-se que $x\ R\ x$, e portanto, pela Definição 3.9 é claro que $Id_A \subset R$.

($\Leftarrow$) Assuma que $Id_A \subset R$, agora uma vez que para todo $x \in A$ tem-se que $(x, x) \in Id_A$, pela Definição 1.5 segue que $(x, x) \in R$, isto é, tem-se que $x\ R\ x$, e portanto, R é reflexiva. □

Corolário 3.2 Uma relação R é reflexiva se, e somente se, R^{-1} é reflexiva.

Demonstração. A demonstração é simples e fica como exercício ao leitor. □

Teorema 3.15 — Fecho Algébrico das Relações Reflexivas. Se R_1 e R_2 são relações reflexivas sobre o mesmo conjunto, então $R_1 \cup R_2$ e $R_1 \cap R_2$ são também relações reflexivas.

Demonstração. Assuma que R_1 e R_2 são relações reflexivas sobre um conjunto A, assim pelo Teorema 3.14 tem-se que $Id_A \subset R_1$ e $Id_A \subset R_2$, agora pelo Teorema 1.3 tem-se a seguinte relação de inclusão:

$$R_1 \subseteq R_1 \cup R_2$$

logo, tem-se que $Id_A \subset R_1 \subseteq R_1 \cup R_2$, consequentemente pelo Teorema 1.3 tem-se que $R_1 \cup R_2$ é uma relação reflexiva. Agora suponha por absurdo que $Id_A \not\subset (R_1 \cap R_2)$, logo existe $(x, x) \in Id_A$ tal que $(x, x) \notin (R_1 \cap R_2)$, consequentemente pela Definição 1.8 tem-se que $(x, x) \notin R_1$ e $(x, x) \notin R_2$, o que contradiz a hipótese de que R_1 e R_2 sejam relações reflexivas, isto é, contradiz a hipótese de $Id_A \subset R_1$ e $Id_A \subset R_2$, e portanto, $Id_A \subset (R_1 \cap R_2)$, logo pelo Teorema 3.14 tem-se que $R_1 \cap R_2$ é também uma relação reflexiva. □

Teorema 3.16 Seja R_1 uma relação reflexiva sobre um conjunto A e seja R_2 um relação qualquer sobre o conjunto A, tem-se $R_1 \cup R_2$ é uma relação reflexiva.

Demonstração. A demonstração é trivial e ficará como exercício ao leitor. □

Teorema 3.17 Se R é uma relação reflexiva, então $R \bullet R^{-1}$ e $R^{-1} \bullet R$ são também relações reflexivas.

Demonstração. Assuma que R é uma relação reflexiva sobre um conjunto A, assim pelo Corolário 3.2 tem-se que R^{-1} é uma relação reflexiva. Assim pelo Teorema 3.14 tem-se que $Id_A \subseteq R$ e $Id_A \subseteq R^{-1}$, consequentemente, pelo Corolário 3.1 tem-se que $(Id_A \bullet Id_A) \subseteq (R \bullet R^{-1})$ e $(Id_A \bullet Id_A) \subseteq (R^{-1} \bullet R)$, mas pela neutralidade da relação identidade (Teorema 3.13) tem-se que $Id_A \bullet Id_A = Id_A$, assim tem-se que $Id_A \subseteq (R \bullet R^{-1})$ e $Id_A \subseteq (R^{-1} \bullet R)$, e portanto, $R \bullet R^{-1}$ e $R^{-1} \bullet R$ são relações reflexivas. □

Teorema 3.18 Se R é uma relação reflexiva, então as seguintes afirmações são verdadeiras.

(i) $R \subset R \bullet R$.

(ii) $R \bullet R$ é reflexiva.

Demonstração. A demonstração é simples e fica como exercício ao leitor. □

Um terceiro tipo de relações binárias é o tipo irreflexivo, de um certo ponto de vista, tal tipo de relação pode ser visto como sendo o contraponto do tipo reflexivo.

Definição 3.11 — Tipo Irreflexivo. Uma relação R é dita ser irreflexiva quando para todo $x \in A$ tem-se que $x \not R\, x$.

Exemplo 3.18 Seja P o conjunto de todas as pessoas, e seja R a relação "ser vó", tem-se que R é irreflexiva pois é claro que ninguém pode ser vó de si próprio, portanto, para todo $x \in P$ tem-se que $x \not R\, x$.

Exemplo 3.19 Seja $\mathbb{N}_1 = \{x \in \mathbb{N} \mid x > 0\}$ tem-se que a relação R definida sobre $\mathbb{N}_1$ como sendo $x \not R\, y \iff y = 2x$ é irreflexiva.

Seguindo com a tipagem das relações binárias, a seguir este manuscrito irá apresentar os tipos: simétrico, assimétrico e anti-simétricos.

Definição 3.12 — Tipo Simétrico. Uma relação R é dita ser simétrica quando para todo $x, y \in A$ se $x \, R \, y$, então $y \, R \, x$.

Exemplo 3.20 Dado o conjunto $A = \{-3, -2, -1, 0, 1, 2, 3, 4\}$ o conjunto $\{(x, y) \in A^2 \mid x + y \geq 6\}$ é claramente uma relação simétrica sobre A.

Exemplo 3.21 Sendo $B = \{1, 2, 3, 4\}$ o conjunto $\{(1, 1), (1, 3), (4, 2), (2, 4), (2, 2), (3, 1)\}$ é claramente uma relação simétrica sobre B.

Pela Definição 3.12 é fácil notar que uma relação R não será simétrica sempre que existir pelo menos um par (x, y) tal que $x \, R \, y$ mas $y \not R\, x$. O próximo resultado estabelece uma caracterização para as relações simétricas.

Teorema 3.19 — Caracterização das Relações Simétricas. Uma relação R será simétrica se, e somente se, $R = R^{-1}$.

Demonstração. ($\Rightarrow$) Suponha que R é simétrica, logo

$$\begin{aligned} (x, y) \in R &\iff (y, x) \in R \\ &\iff (x, y) \in R^{-1} \end{aligned}$$

portanto, pela Definição 1.6 tem-se que $R = R^{-1}$. ($\Leftarrow$) É trivial e fica como exercício ao leitor. $\square$

Corolário 3.3 Se R é simétrica, então $R \bullet R^{-1} = R^{-1} \bullet R$.

Demonstração. Direto do Teorema 3.19. $\square$

Agora será mostrado que união e interseção são operações fechadas sobre o conjunto de todas as relações binárias simétricas.

Teorema 3.20 Se R e S são relações simétricas, então $R \cup S$ e $R \cap S$ também são simétricas.

Demonstração. Trivial. $\square$

Teorema 3.21 Se R é uma relação qualquer, então $R \bullet R^{-1}$ e $R^{-1} \bullet R$ são ambas simétricas.

Demonstração. Suponha que R é uma relação, assim tem-se que

$$\begin{aligned} (R \bullet R^{-1})^{-1} &\overset{Teo.3.8}{=} (R^{-1})^{-1} \bullet R^{-1} \\ &= R \bullet R^{-1} \end{aligned}$$

e

$$\begin{aligned} (R^{-1} \bullet R)^{-1} &\overset{Teo.3.8}{=} R^{-1} \bullet (R^{-1})^{-1} \\ &= R^{-1} \bullet R \end{aligned}$$

assim pelo Teorema 3.19 tem-se que $R \bullet R^{-1}$ e $R^{-1} \bullet R$ são ambas simétricas. $\square$

Teorema 3.22 Se R é uma relação qualquer, então $R \cup R^{-1}$ e $R \cap R^{-1}$ são ambas simétricas.

Demonstração. Suponha que R é uma relação, assim tem-se que

$$\begin{aligned} (R \cup R^{-1})^{-1} &\overset{Teo.3.12}{=} R^{-1} \cup (R^{-1})^{-1} \\ &= (R^{-1})^{-1} \cup R^{-1} \\ &= R \cup R^{-1} \end{aligned}$$

e

$$\begin{aligned}
(R \cap R^{-1})^{-1} &\overset{Teo.3.12}{=} R^{-1} \cap (R^{-1})^{-1} \\
&= (R^{-1})^{-1} \cap R^{-1} \\
&= R \cap R^{-1}
\end{aligned}$$

assim pelo Teorema 3.19 tem-se que $R \cup R^{-1}$ e $R \cap R^{-1}$ são ambas simétricas. □

Definição 3.13 — Tipo Assimétrico. Uma relação R é dita ser assimétrica quando para todo $x, y \in A$ se $x \; R \; y$, então $y \not R \; x$.

Exemplo 3.22 Considere que P é a relação de paternidade definida sobre o conjunto dos seres humanos, isto é, $x \; P \; y$ significa que x é pai de y, obviamente esta relação é assimétrica pois dado que um indivíduo x é pai de um certo y é impossível que y seja pai de x, ou seja, sempre que $x \; R \; y$ será verdade que $y \not R \; x$.

Exemplo 3.23 A relação $R = \{(x, y) \in \mathbb{N} \mid x - y \leq 0\}$ é uma relação assimétrica

O leitor deve ficar atento ao fato de que uma relação R será dita não ser assimétrica se existir pelo menos um par (x, y) tal que $x \; R \; y$ e também que $x \; R \; y$.

Exemplo 3.24 Considere $K = \{1, 2, 3, 4\}$ e T a relação binária definida sobre o conjunto K tal que $T = \{(1, 2), (1, 3), (4, 1), (1, 4), (2, 3)\}$. Tem-se claramente que T não é assimétrica pois $4 \; T \; 1$ e $1 \; T \; 4$.

O resultado exposto a seguir mostra que o tipo assimétrico e o tipo irreflexivo estão intimamente ligados entre si.

Teorema 3.23 Se R é uma relação assimétrica sobre A, então R é uma relação irreflexiva sobre A.

Demonstração. Suponha por absurdo que R é uma relação assimétrica sobre A e R não é irreflexiva sobre A, logo por R não ser irreflexiva existe $x \in A$ tal que $x \; R \; x$, mas isso não satisfaz a Definição 3.13 e, portanto, isso contradiz a hipótese de que R é uma relação assimétrica sobre A, consequentemente se R é assimétrica, então R tem que ser irreflexiva. □

Definição 3.14 — Tipo Anti-simétrico. Uma relação R é dita ser anti-simétrica quando para todo $x, y \in A$ se $x \; R \; y$ e $y \; R \; x$, então $x = y$.

Exemplo 3.25 Considerando $A = \{1, 2, 3, 4\}$ e $R = \{(1, 1), (2, 3), (4, 4), (4, 3)\}$ tem-se que R é claramente anti-simétrica.

Exemplo 3.26 Dado um conjunto A qualquer a relação de subconjunto $\subseteq$ sobre $\wp(A)$ é uma relação que é anti-simétrica, pois para todo $A, B \in \wp(A)$ quando $A \subseteq B$ e $B \subseteq A$ tem-se por definição que $A = B$.

O leitor deve ter notado que uma relação R sobre um conjunto A não será anti-simétrica se existir pelo menos $x, y \in A$ tais que $x \; R \; y$ e $y \; R \; x$, mas $x \neq y$.

Exemplo 3.27 Considere que $A = \{1, 2, 3, 4\}$ e $R = (1, 1), (3, 2), (2, 3), (3, 4)$ obviamente R não é anti-simétrica pois $3 \; R \; 2$ e $2 \; R \; 3$ mas claramente 2 e 3 são elementos distintos de A.

Teorema 3.24 — Caracterização das Relações Anti-simétricas. Uma relação R é anti-simétrica sobre A se, e somente se, $R \cap R^{-1} \subset Id_A$.

Demonstração. ($\Rightarrow$) Suponha por absurdo que R é anti-simétrica sobre A e que $R \cap R^{-1} \not\subset Id_A$, logo existe $(x, y) \in R \cap R^{-1}$ tal que $(x, y) \notin Id_A$, mas pelo fato de que $(x, y) \in R \cap R^{-1}$ tem-se que $(x, y) \in R$ e $(x, y) \in R^{-1}$ e assim $(y, x) \in R$ e como R é anti-simétrica tem-se que $x = y$, logo $(x, y) \in Id_A$ o que é um absurdo, portanto, se R é anti-simétrica sobre A, então tem-se que $R \cap R^{-1} \subset Id_A$. ($\Leftarrow$) Suponha que $R \cap R^{-1} \subset Id_A$, assim seja $x, y \in A$ tal que $x \; R \; y$ e $y \; R \; x$, ou seja, $(x, y) \in R$ e $(x, y) \in R^{-1}$, logo $(x, y) \in R \cap R^{-1}$ e assim tem-se que $x = y$ e assim R é anti-simétrica. $\square$

Corolário 3.4 Uma relação R é anti-simétrica se, e somente se, R^{-1} for anti-simétrica.

Demonstração. Note que,

$$
\begin{aligned}
R \text{ é uma relação anti-simétrica} \quad & \overset{Teo. 3.24}{\iff} \quad R \cap R^{-1} \subset Id_A \\
& \overset{Teo. 3.6}{\iff} \quad (R \cap R^{-1})^{-1} \subset Id_A^{-1} \\
& \overset{Prop. 3.3}{\iff} \quad (R \cap R^{-1})^{-1} \subset Id_A \\
& \overset{Teo. 3.12(2)}{\iff} \quad R^{-1} \cap (R^{-1})^{-1} \subset Id_A \\
& \overset{Teo. 3.24}{\iff} \quad R^{-1} \text{ é uma relação anti-simétrica}
\end{aligned}
$$

E isto conclui a prova. $\square$

Teorema 3.25 Se R e S são relações anti-simétricas, então $R \cap S$ também é anti-simétrica.

Demonstração. Suponha que R e S são relações anti-simétricas, logo pela Teorema

3.24 tem-se que $R \cap R^{-1} \subset Id_A$ e $S \cap S^{-1} Id_A$, agora note que,

$$\begin{aligned}
(R \cap S) \cap (R \cap S)^{-1} &\overset{Teo.3.12(2)}{=} (R \cap S) \cap (R^{-1} \cap S^{-1}) \\
&\overset{Tab.1.1(p2)\ e\ (p3)}{=} (R \cap R^{-1}) \cap (S \cap S^{-1}) \\
&\overset{Hip.}{\subset} Id_A \cap Id_A \\
&= Id_A
\end{aligned}$$

Portanto, $(R \cap S) \cap (R \cap S)^{-1} \subset Id_A$ e assim pelo Teorema 3.24 tem-se que $R \cap S$ é anti-simétrica. □

Continuando a apresentação dos tipos (propriedades) das relações binárias, agora será introduzida o tipo transitivo.

Definição 3.15 — Tipo Transitivo. Uma relação R é dita ser transitiva quando para todo $x, y, z \in A$ se $x\ R\ y$ e $y\ R\ z$, então $x\ R\ z$.

Exemplo 3.28 Dado um conjunto não vazio A a relação $\subseteq$ definida sobre $\wp(A)$ é um clássico exemplo de relação transitiva.

Exemplo 3.29 A relação $R = \{(x, y) \in \mathbb{R}^2 \mid (\exists k \in \mathbb{R})[x = ky]\}$ é uma relação transitiva[a].

[a] A prova disso ficará como exercício ao leitor.

Exemplo 3.30 A relação "ser ancestral de", definida sobre o conjunto de todos os seres humanos (vivos e mortos) é uma relação transitiva.

Como muito explicado em [1] uma relação não será transitiva sempre que existirem $x, y, z \in A$ tais que $x\ R\ y$ e $y\ R\ z$ mas $x \not R\ z$.

Exemplo 3.31 Seja $P = \{1, 2, 3, 4\}$ a relação $R_1 = \{(1, 1), (1, 2), (2, 4), (3, 2), (1, 4)\}$ é transitiva, já a relação $R_2 = \{(1, 1), (3, 1), (1, 2), (2, 3), (2, 4), (3, 3), (4, 1)\}$ não é transitiva pois $(3, 1), (1, 2) \in R_2$ mas $(3, 2) \notin R_2$.

Teorema 3.26 — Caracterização das Relações Transitivas. Uma relação R é transitiva sobre A se, e somente se, $R \bullet R \subset R$.

Demonstração. ($\Rightarrow$) Suponha que R seja transitiva, assim para todo $(x, y), (y, z) \in R$ é tal que $(x, z) \in R$, mas note que $(x, y), (y, z) \in R$ implica que $(x, z) \in R \bullet R$ e, portanto, $R \bullet R \subseteq R$. ($\Leftarrow$) Assuma que $R \bullet R \subset R$, logo todo $(x, z) \in R \bullet R$ é tal que $(x, z) \in R$, mas note que $(x, z) \in R \bullet R$ implica que existe $y \in A$ tal que $(x, y), (y, z) \in R$ e assim por definição R é transitiva. □

Corolário 3.5 Uma relação R é transitiva se, e somente se, R^{-1} é também transitiva.

Demonstração. Note que,

$$\begin{aligned}
R \text{ é uma relação transitiva} \quad & \overset{Teo.3.26}{\iff} \quad R \bullet R \subset R \\
& \iff \quad (R \bullet R)^{-1} \subset R^{-1} \\
& \overset{Teo.3.8}{\iff} \quad R^{-1} \bullet R^{-1} \subset R^{-1} \\
& \overset{Teo.3.26}{\iff} \quad R^{-1} \text{ é uma relação transitiva}
\end{aligned}$$

E isto conclui a prova. □

Teorema 3.27 Se R é transitiva, então $R \bullet R$ é transitiva.

Demonstração. Direto do Teorema 3.26. □

Por fim será agora apresentado o último tipo das relação binárias, sendo este último tipo a contraparte do tipo transitivo.

Definição 3.16 — Tipo Intransitivo. Uma relação R é dita ser intransitiva quando para todo $x, y, z \in A$ se $x \; R \; y$ e $y \; R \; z$, então $x \not R \; z$.

Exemplo 3.32 A relação "x é mãe de y" definida sobre o conjunto de todas as pessoas (vivas e mortas) é uma relação intransitiva, pois se "Maria é mãe de Julia" e "Julia é mãe de Rebeca" tem-se que "Maria não pode ser mãe de Rebeca".

O leitor atento pode notar que uma relação R sobre um conjunto não vazio A qualquer, será dita não ser intransitiva quando existir pelo menos três elementos $x, y, z \in A$ tal que $x \; R \; y$ e $y \; R \; z$ e $x \; R \; z$.

3.5 Fecho das Relações Binárias

Dado uma relação R e uma propriedade P não satisfeita por R, pode-se questionar "É possível fazer R satisfazer P?", a resposta para essa pergunta é clara, **não**! Pois R, é uma estrutura matemática (uma relação) o que significa que é imutável[4]! O que se pode fazer neste caso, como explicando em [28], é criar uma nova relação R' que seja o fecho-P de R, ou seja, essa nova relação é como uma cobertura que fecha R com respeito a propriedade P.

A seguir, seguindo a ordem de apresentação vista em [60], este documento irá apresentar de forma direta como é possível fechar as relações com respeito as propriedades de reflexividade, simetria e transitividade, ou seja, serão definidos os "algoritmos" de fechamento para tais propriedades.

[4]Em matemática os objetos são imutáveis no sentido de que, eles são como são, desde o momento de sua "criação", ou seja, não existe liberdade para mudar de comportamento ou as propriedades dos elementos.

Definição 3.17 — Fecho de uma relação. Seja R uma relação sobre A e P uma propriedade, a relação $\widehat{R}$ definida sobre A é dita ser o fecho de R com respeito a P sempre que:

1. $\widehat{R}$ possui a propriedade P.
2. $R \subseteq \widehat{R}$.
3. Para toda relação R^* que satisfaça as condições (1) e (2) tem-se que $\widehat{R} \subseteq R^*$.

Para fins de interesse de estudantes de computação e também para fins didáticos neste manuscrito serão estudados os métodos de construção dos fechos para propriedades específicas, a saber, as propriedades de reflexividade, transitividade e simetria.

Observação 3.3 — O ponto fixo! ALiCIA chama sua atenção para o fato de que se R já possui uma certa propriedade P, o fecho de R com respeito a esta propriedade P será exatamente o próprio R. Nesta situação é dito que R é o ponto fixo de R com respeito a P.

Definição 3.18 Seja R uma relação binária sobre A o fecho reflexivo de R, denotado por $ref(R)$, corresponde a seguinte relação:

$$ref(R) = R \cup Id_A$$

Exemplo 3.33 Seja $A = \{a, b, c\}$ e $R = \{(a, a), (a, b), (a, c), (c, a), (b, c)\}$ uma relação sobre A, o fecho reflexivo desta relação é dado por:

$$\begin{aligned} ref(R) &= R \cup Id_A \\ &= \{(a, a), (a, b), (a, c), (c, a), (b, c)\} \cup \{(a, a), (b, b), (c, c)\} \\ &= \{(a, a), (a, b), (a, c), (c, a), (b, c), (b, b), (c, c)\} \end{aligned}$$

Exemplo 3.34 Seja $B = \{0, 1\}$ e $K = \{(0, 0), (1, 0), (0, 1)\}$ uma relação sobre B, o fecho reflexivo desta relação é dado por:

$$\begin{aligned} ref(K) &= R \cup Id_B \\ &= \{(0, 0), (1, 0), (0, 1)\} \cup \{(0, 0), (1, 1)\} \\ &= \{(0, 0), (1, 0), (0, 1), (1, 1)\} \end{aligned}$$

Exemplo 3.35 Dado o conjunto $\mathbb{N}$ e a relação "menor que" definida nos números naturais corresponde ao conjunto $\{(x,y) \in \mathbb{N}^2 \mid (\exists z \in \mathbb{N}_*)[x = y + k]\}$ e o fecho reflexivo para tal relação é exatamente a relação "menor ou igual que" e corresponde exatamente ao conjunto $\{(x,y) \in \mathbb{N}^2 \mid (\exists z \in \mathbb{N})[x = y + k]\}$.

Definição 3.19 Seja R uma relação binária sobre A o fecho simétrico de R, denotado por $sim(R)$, corresponde a seguinte relação:

$$sim(R) = R \cup \{(y,x) \mid (x,y) \in R\}$$

Exemplo 3.36 Seja $A = \{a,b,c\}$ e $R = \{(a,a),(a,b),(a,c),(c,a),(b,c)\}$ uma relação sobre A, o fecho reflexivo desta relação é dado por:

$$\begin{aligned} sim(R) &= R \cup \{(y,x) \mid (x,y) \in R\} \\ &= \{(a,a),(a,b),(a,c),(c,a),(b,c)\} \cup \{(a,a),(b,a),(c,a),(a,c),(c,b)\} \\ &= \{(a,a),(a,b),(a,c),(c,a),(b,c),(b,a),(c,b)\} \end{aligned}$$

Exemplo 3.37 Se X é o conjunto dos humanos (vivos ou mortos) e M é a relação "pai de", então $sim(M) = \{(x,y) \in X^2 \mid x$ é pai de y ou y é filho de $x\}$.

O próximo fecho apresentado é chamado de fecho transitivo, de um ponto de vista de teoria dos grafos, é exibição direta da propriedade de caminho entre dois pontos A e B, sem, entretanto, necessitar informar a existência dos pontos e caminhos intermediários que ligam A e B.

Definição 3.20 Seja R uma relação binária sobre A o fecho transitivo de R, denotado por R^+, corresponde a seguinte relação:

$$R^+ = \bigcup_{i=1}^{\infty} R_i$$

em que, $R^1 = R$ e $R^{i+1} = R \bullet R^i$. Em particular, quando A for um conjunto finito a igualdade acima pode ser reescrita como:

$$R^+ = \bigcup_{i=1}^{n} R_i$$

O fecho transitivo é especialmente importante para diversas áreas que são usualmente de interesse dos cientistas da computação tais como a teoria dos grafos, a lógica e teoria da complexidade. Particularmente o fecho transitivo aparece de forma recorrente nos algoritmos de banco de dados, como dito em [60], pois diversos bancos de dados são construídos desde a década de 70 de forma que seja sempre possível realizar a implementação de fechos transitivos.

Exemplo 3.38 Para qualquer conjunto A a relação binária $\subseteq$ definida sobre $\wp(A)$ é um clássico exemplo de relação cujo fecho transitivo é igual a ela mesmo.

Exemplo 3.39 Dado o conjunto $B = \{0, 1\}$ e a relação $T = \{(1, 0), (0, 1)\}$ definida sobre B tem-se que o fecho transitivo de T é dado por,

$$\begin{aligned}
T^+ &= \bigcup_{i=1}^{2} T_i \\
&= T_1 \cup T_2 \\
&= T \cup (T \bullet T_1) \\
&= T \cup (T \bullet T) \\
&= \{(1,0),(0,1)\} \cup \{(1,0),(0,1),(1,1),(0,0)\} \\
&= \{(1,0),(0,1),(1,1),(0,0)\}
\end{aligned}$$

Exemplo 3.40 Seja $A = \{1, 2, 3\}$ e $S = \{(1, 2), (2, 2), (3, 1), (2, 3)\}$ uma relação sobre A o fecho transitivo de R é exatamente o conjunto:

$$\begin{aligned}
S^+ &= \bigcup_{i=1}^{3} S_i \\
&= S_1 \cup S_2 \cup S_3 \\
&= S \cup (S \bullet S_1) \cup (S \bullet S_2) \\
&= \{(1,2),(2,2),(3,1),(2,3),(1,3),(1,1),(3,3)\}
\end{aligned}$$

3.6 Relações e Grafos

Escrever depois...

3.7 Questionário

Questão 3.1 Dado os conjuntos $A = \{1, 2, 3\}, B = \{x, y\}, C = \{q, v\}$ e $D = \{-1, 0, 1\}$ construa os conjuntos a seguir.

(a). $A \times B$.

(b). $A \times C$.

(c). $B \times D$.

(d). $C \times A$.

(e). $A \times A$.

(f). $A \times (B \times D)$.

(g). $((A \times B) \cap (D \times A)) \times C$.

(h). $C \times ((B \times A) \cap (A \times D))$.

(i). $B^3 \times D^2$.

(j). $A^2 \times (C^3 \times D)$.

(k). $A \times B \times C$.

(l). $A \times (B \times C)$.

(m). $A^2 \times (B \times C)$.

(n). $(D^3 \times C) \times B$.

(o). $A^2 \times A^2$.

Questão 3.2 Considerando $X = \{1, 2\}, Y = \{a, b\}$ e $Z = \{b, c\}$ determine:

(a). $X \times (Y \cup Z)$.

(b). $X \times (Y - Z)$.

(c). $(X \times Y) \times Z$.

(d). $(X \times Z) \times Y$.

(e). $X \times (Y \ominus Z)$.

(f). $X \times (Y \cap Z)$.

(g). $(X \times Y) \times (X \times Z)$.

(h). $(X \times Y) \cap (X \times Z)$.

(i). $X^2 \times Y^2$

(j). $Z^2 \times Y^2$

Questão 3.3 Sendo $(x + y, 1), (3, x - y) \in \mathbb{N}^2$ dado que $(x + y, 1) = (3, x - y)$, determine o valor de x e y.

Questão 3.4 Dado os conjuntos $A = \{P, R\}, B = \{N, E\}$ e $C = \{1, 2\}$ construa os diagramas de árvore para os seguintes produtos Cartesianos.

(a). A^2.

(b). $B \times C$.

(c). $A \times (B \times C)$.

(d). $B \times (A \times C)$.

(e). $C^2 \times B$.

(f). $C^3 \times C$.

(g). $A \times C^2$.

(h). $B \times (C \cup A)$.

(i). $(A \cup C)^2 \times A$.

(j). $A^2 \times B \times C^2$.

Questão 3.5 Determine o domínio e a imagem das seguintes relações binárias.

(a). $R_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq x, y \leq 6, y = 2x\}$[5].

(b). $R_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq x \leq 5, 1 \leq y \leq 4, (x - y) \in \mathbb{N}\}$.

(c). $R_3 = \{(a, b), (e, c), (a, c), (o, c), (i, (d, f)), ((o, u), b), ((o, u), c), (u, b)\}$.

(d). $R_4 = \{(x_0, x_1) \mid x_0$ é uma concoante e x_1 é uma vogal$\}$.

(e). $R_5 = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x + x = x, x + y = y\}$.

Questão 3.6 Determine o domínio, imagem e a relação inversa das seguintes relações binárias.

(a). Relação igualdade sobre o conjunto $\mathbb{N}_1$ com $\mathbb{N}_1 = \{x \in \mathbb{N} \mid x > 0\}$.

(b). Relação "maior que" sobre o conjunto $\{1, 2, 3, 4, 5, 6\}$.

(c). Relação $\subseteq$ sobre um conjunto $\wp(A)$ com A sendo um conjunto arbitrário.

Questão 3.7 Dado os pares ordenados:

$$\begin{array}{rcl}
(6,4),(2,3), & (3,-3), & (9,3),(3,3), \\
(4,5),(3,1), & (7,4), & (2,4),(1,8), \\
(-1,1),(0,5), & (9,3), & (8,11), \\
(-1,2),(4,-6), & (1,2), & (10,-5),(0,0), \\
(4,0),(9,3), & (5,0), & (0,1),(3,1)
\end{array}$$

Para cada relação definida sobre os inteiros a seguir diga quais pares pertencem as relações.

(a). $A = \{(x, y) \mid x + 2y > 15\}$.

(b). $B = \{(x, y) \mid xy \geq 8\}$.

(c). $C = \{(x, y) \mid (\exists k \in \mathbb{N})[x + y = 2k]\}$.

(d). $D = \{(x, y) \mid (\exists k \in \mathbb{N})[k = \sqrt{xy}]\}$.

[5] Na relação $\leq$ quando é escrito que $0 \leq x, y \leq z$ significa que ambas as desigualdades $0 \leq x \leq z$ e $0 \leq y \leq z$ são verdadeiras, porém, não se tem qualquer informação acerca da tricotomia entre os elementos x e y.

(e). $E = \{(x, y) \mid (\exists k \in \mathbb{N})[x^y = 2k]\}$.

(f). $F = \{(x, y) \mid x, y$ são múltiplos de $5\}$.

(g). $R = \{(x, y) \mid x + y < 9\}$.

(h). $S = \{(x, y) \mid 3x + y < 15\}$.

(i). $T = \{(x, y) \mid 3x + 2y = 10\}$.

(j). $U = \{(x, y) \mid (\exists k \in \mathbb{N})[y = \sqrt{k}]\}$.

(k). $V = \{(x, y) \mid x - y \in \mathbb{N}\}$.

(l). $X = \{(x, y) \mid x, y$ são primos$\}$.

(m). $Y = \{(x, y) \mid mmc(x, y) = 4\}$.

(n). $Z = \{(x, y) \mid 2x - y = x\}$.

Questão 3.8 Para cada relação a seguir diga se ela é reflexiva, simétrica, transitiva ou que não tem nenhuma destas propriedades (ou tipos).

(a). $R_1 = \{(a, a), (a, b), (a, d), (b, b), (b, a), (c, d), (d, d)\}$.

(b). $R_2 = \{(a, a), (b, a), (b, b), (b, c), (c, c), (c, d)\}$.

(c). $R_3 = \{(d, d), (c, d), (d, c)\}$.

(d). $R_4 = \{(b, c), (c, b), (b, d), (d, b)\}$.

(e). $R_5 = \{(a, a), (a, b), (a, c), (b, c)\}$.

(f). $R_6 = \{(a, b), (a, c)\}$.

(g). $R_7 = \{(a, d), (c, d)\}$.

(h). $R_8 = \{(a, a), (b, b)\}$.

Questão 3.9 Para cada relação do Exercício 3.7 diga se ela é reflexiva, simétrica, transitiva ou que não tem nenhuma destas propriedades (ou tipos).

Questão 3.10 Considere o universo do discurso $\mathbb{U} = \{a, b, c\}$ verifique se as seguintes relações definidas sobre $\mathbb{U}$ são reflexivas, simétricas, antissimétricas ou transitivas.

(a). $S_1 = \{(a, c), (c, c), (c, a), (b, b), (b, c), (1, 1), (1, 2)\}$.

(b). $S_2 = \{(a, a), (c, c), (b, b), (b, c)\}$.

(c). $S_3 = \{(a, a), (a, b), (b, c), (c, a), (a, c)\}$.

(d). $S_4 = \{(a, a), (a, b), (b, c), (a, c)\}$.

Questão 3.11 Considere o universo do discurso $\mathbb{U} = \{a, b, c, d, e, f\}$ verifique se as seguintes relações definidas sobre $\mathbb{U}$ são reflexivas, simétricas, antissimétricas ou transitivas.

(a). $T = \{(a, a), (b, b), (c, c), (e, e), (f, f), (a, b), (b, c), (c, e), (e, f)\}$.

(b). $U = \{(a, b), (b, a), (c, e), (e, c), (e, f), (f, e)\}$.

(c). $V = \{(a, b), (b, c), (a, c), (c, a), (c, b), (b, a), (a, a), (b, b), (c, c)\}$.

(d). $X = \{(a, a), (b, b), (c, c), (e, e), (f, f), (e, f), (f, e)\}$.

(e). $Y = \emptyset$.

Questão 3.12 Esboce a relação inversa de cada uma das relações dos Exercícios 3.10 e 3.11.

Questão 3.13 Considere o universo do discurso $\mathbb{U} = \{1, 2, 0, 4\}$ e construa sobre $\mathbb{U}$:

(a). Uma relação que seja reflexiva e transitiva, mas não seja simétrica.

(b). Uma relação que seja reflexiva e simétrica, mas não seja transitiva.

(c). Uma relação que seja simétrica e transitiva, mas não seja reflexiva.

(d). Uma relação que não seja reflexiva e nem transitiva, e também não seja simétrica.

Questão 3.14 Esboce os fechos reflexivo, simétrico e transitivo de cada relação no Exercício 3.10.

Questão 3.15 Esboce os fechos reflexivo, simétrico e transitivo de cada relação no Exercício 3.11.

Capítulo 4

Equivalência e Ordem

> *"O problema do mundo hoje é que as pessoas inteligentes estão cheias de dúvidas, e as pessoas idiotas estão cheias de certezas..."*
>
> *Bertrand Russell*

4.1 Introdução

No Capítulo 3 anterior este documento apresentou ao leitor a ideia de relações sobre conjuntos, em especial foram tratadas as relações binários sobre um conjunto dado. Agora nesta seção será apresentada de forma profunda duas classes relações binárias muito importantes, sendo elas as relações de equivalência e de ordem. Como dito em [1, 14], as relações de equivalência ao lado das relações de ordem são de importância central para toda a matemática, além disso, as relações de equivalência também desempenho importantes papéis nas área de mineração de dados [41, 42], aprendizado de máquina [4] e processamento de sinais [40] e imagens [2, 57]. E por sua vez, as relações de ordem também aparecem em diversas áreas de caráter prática tais como processamento de imagens [25, 20], criptografia [29], otimização [35] e etc.

4.2 Relações de Equivalência e Espaço Quociente

E interessante começar pela pergunta básica, o que seria uma relação de equivalência? Bem, uma resposta satisfatória para essa pergunta é que uma relação de equivalência pode ser entendida como sendo uma forma de parear os elementos de um conjunto que apresentam similaridade entre si com respeito a uma ou mais propriedades específicas, isto é, uma relação de equivalência junta os elementos em pares pela similaridade, definida por algum critério. A seguir será apresentado de forma precisa o conceito de relação de equivalência.

Definição 4.1 — Relação de Equivalência. Seja A um conjunto uma relação binária $\equiv$ sobre A é dita ser uma relação de equivalência sempre que $\equiv$ for reflexiva, simétrica e transitiva.

Tomando Notas 4.1 – Sobre notação ALicia chama sua atenção para o fato que além da notação $\equiv$ outros símbolos também são comumente encontrados na literatura para representar relações de equivalência, entre, tais símbolos destacam-se $\approx$ e $\sim$.

Exemplo 4.1 Dado um conjunto C qualquer, a relação de igualdade $(=)$ definida em C é obviamente uma relação de equivalência.

Exemplo 4.2 Dado o conjunto $A = \{a, b, c, d\}$ a relação R definida por $a\ R\ a$, $a\ R\ b$, $b\ R\ a$, $b\ R\ b$, $c\ R\ c$ e $d\ R\ d$, é claramente uma relação de equivalência.

Os Exemplos 4.1 e 4.2 permite o leitor perceber uma importante verdade matemática, tal verdade como expressa em [14] pode ser escrita como: "objetos iguais são equivalentes, mas objetos equivalentes nem sempre são iguais".

Exemplo 4.3 Dado um plano P a relação de paralelismo definido sobre o conjunto de retas de P é uma relação de equivalência, outro exemplo clássico da geometria é a semelhança entre triângulos neste mesmo plano P.

Exemplo 4.4 A relação $R = \{(x, y) \in \mathbb{Z}^2 \mid x \mod 5 = y \mod 5\}$ é uma relação de equivalência[a].

[a] A expressão $a \mod 5$ com $a \in \{x, y\}$ diz respeito ao resto da divisão inteira de a por 5.

Exemplo 4.5 A relação $I = \{(x, y) \in PERS^2 \mid x, y$ possuem a mesma idade$\}$ é uma relação de equivalência sobre o conjunto de todas as pessoas $(PERS)$.

Exemplo 4.6 Dado o conjunto de todos os times de futebol do Brasil a relação T definida como $x\ T\ y \iff x, y$ nunca foram rebaixados para a segunda divisão, é uma relação de equivalência.

A partir da noção de relação de equivalência é possível como destacado em [1] definir a noção de classes de equivalência.

Definição 4.2 — Classes de Equivalência. Seja $\equiv$ uma relação de equivalência sobre um conjunto A, para todo $x \in A$ é definida a classe de equivalência de x, denotado por $[x]$, como sendo o conjunto de todos os elementos equivalentes a x, simbolicamente tem-se que:

$$[x] = \{y \in A \mid y \equiv x\}$$

Obviamente toda classe de equivalência $[x]$ é um subconjunto do conjunto base[1]. Além disso, obviamente tem-se que $[x] = \emptyset$ se, e somente se, o conjunto base for vazio.

Exemplo 4.7 Seja $A = \{0, 1, 2, 3\}$ e $0 \equiv 0$, $1 \equiv 1$, $2 \equiv 2$, $3 \equiv 3$, $0 \equiv 2$, $1 \equiv 3$, $2 \equiv 0$, $3 \equiv 1$ tem-se que: $[0] = \{0, 2\}$, $[1] = \{1, 3\}$, $[2] = \{0, 2\}$ e $[3] = \{1, 3\}$.

Exemplo 4.8 A relação $a \equiv a$, $b \equiv b$, $c \equiv c$, $a \equiv b$, $b \equiv a$ definida sobre o conjunto $\{a, b, c\}$ é uma relação de equivalência e existem as seguintes classes de equivalência $[a] = [b] = \{a, b\}$ e $[c] = \{c\}$.

Teorema 4.1 Seja $\equiv$ uma relação de equivalência sobre um conjunto A não vazio e sejam $a, b \in A$, tem-se que $a \equiv b$ se, e somente se, $[a] = [b]$.

Demonstração. ($\Rightarrow$) Suponha que $a \equiv b$, assim dado qualquer $x \in [a]$ tem-se que $x \equiv a$, agora pela transitiva de $\equiv$ é claro que $x \equiv b$ e, portanto, $x \in [b]$, logo $[a] \subseteq [b]$ e com raciocínio similar pode-se concluir que $[b] \subseteq [a]$ e assim pela Definição 1.6 tem-se que $[a] = [b]$. ($\Leftarrow$) Suponha que $[a] = [b]$, por $\equiv$ ser reflexiva é claro que $a \equiv a$ e assim $a \in [a]$, mas como $[a] = [b]$ tem-se que $a \in [b]$, e portanto, por definição $a \equiv b$. $\square$

Teorema 4.2 Seja $\equiv$ uma relação de equivalência sobre um conjunto A não vazio e sejam $a, b \in A$, tem-se que $a \not\equiv b$ se, e somente se, $[a] \cap [b] = \emptyset$.

Demonstração. ($\Rightarrow$) Suponha por absurdo que $a \not\equiv b$ e $[a] \cap [b] \neq \emptyset$, logo existe um $x \in A$ tal que $x \in [a] \cap [b]$, mas assim pela Definição 1.8 tem-se que $x \in [a]$ e $x \in [b]$, logo $x \equiv a$ e $y \equiv b$, mas uma vez que $\equiv$ é simétrica tem-se que $a \equiv x$, e como $\equiv$ é transitiva tem-se que $a \equiv b$, o que contradiz a hipótese, caraterizando um absurdo, consequentemente, se $a \not\equiv b$ tem-se então que $[a] \cap [b] = \emptyset$. ($\Leftarrow$) Suponha que $[a] \cap [b] = \emptyset$, como $a \in [a]$ e pela hipótese $a \notin [a] \cap [b]$ tem-se que $a \notin [b]$ e, portanto, $a \not\equiv b$. $\square$

[1] Conjunto base aqui, assim como no Capítulo 3, diz respeito ao conjunto sobre o qual a relação de equivalência está definida.

Definição 4.3 — Espaço Quociente. Seja A um conjunto e $\equiv$ uma relação de equivalência sobre A, o espaço quociente de A com respeito (ou módulo) $\equiv$, denotado por $A_{/\equiv}$, é o conjunto de todas as classes de equivalência do conjunto A, na linguagem na teoria dos conjuntos tem-se que:

$$A_{/\equiv} = \{[x] \mid x \in A\}$$

Exemplo 4.9 Seja $A = \{a, b, c\}$ e $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ claramente R é uma relação de equivalência e além disso $[a] = [b] = \{a, b\}$ e $[c] = \{c\}$ assim $A_{/R} = \{[a], [c]\}$.

Exemplo 4.10 Dado que a relação

$$P = \{(x, y) \in \mathbb{Z}_+ \mid x, y \text{ tem o mesmo resto da divisão por } 2\}$$

é uma relação de equivalência sobre $\mathbb{Z}_+$ (a prova fica como exercício ao leitor) tem-se claramente que,

$$[0] = \{0, 2, 4, 6, 8, \cdots\}$$

e

$$[1] = \{1, 3, 5, 7, 9, \cdots\}$$

ou seja, $[0]$ é o conjunto dos pares positivos e $[1]$ é o conjunto dos impares positivos, assim claramente tem-se que $\mathbb{Z}_{+/P} = \{[0], [1]\}$.

Uma fato importante sobre o espaço quociente de uma relação de equivalência $\equiv$ é que sempre que o conjunto base $A \neq \emptyset$ tem-se que $A_{/\equiv} \neq \emptyset$, e mais do que isso, como mostrado a seguir o espaço quociente é sempre uma partição sobre o conjunto base A.

Teorema 4.3 Seja $\equiv$ uma relação de equivalência sobre um conjunto não vazio A, então $A_{/\equiv}$ é uma partição de A.

Demonstração. Primeiramente note que como $\equiv$ é uma relação reflexiva tem-se para todo $x \in A$ que $x \in [x]$ e assim claramente $[x] \in A_{/\equiv}$ e $[x] \neq \emptyset$, satisfazendo assim a condição (1) da Definição 1.14. Por outro lado, os Teoremas 4.1 e 4.2 mostram que dado $[x], [y] \in A_{/\equiv}$ sempre que $[x] \neq [y]$ tem-se que $[x] \cap [y] = \emptyset$ e, portanto, a condição (2) da Definição 1.14 é satisfeita, desde que as condições (1) e (2) são satisfeita pelo elementos de $A_{/\equiv}$ tem-se que $A_{/\equiv}$ é uma partição de A. $\square$

4.3 Relações de Ordem

Em algumas situações é interessante que seja possível definir uma hierarquia entre os elementos de um determinado conjunto, de fato, como dito em [1] diversos campos das ciências empíricas, tais como a área da biologia comparada, são dependentes de construções hierárquicas. Dentro da própria ciência da computação diversas áreas (estrutura de dados, classificação de dado e etc.) também utilizam de ordens de hierarquia. Assim é conveniente apresentar o estudo das relações de ordem e das estruturas existentes envolta de tais relações, para isso apresenta-se primeiro as ideias de pré-ordem e ordem estrita.

Definição 4.4 — Ordem Estrita. Seja A um conjunto, uma relação $\sqsubset$ sobre A, é dita ser uma relação de ordem parcial estrita, ou simplesmente ordem estrita, sempre que $\sqsubset$ for irreflexiva e transitiva.

Exemplo 4.11 A relação $\{(x, y) \in \mathbb{N}^2 \mid (\exists k \in \mathbb{N})[k \geq 1 \wedge y = x + k]\}$ é uma ordem estrita.

Exemplo 4.12 Dado um conjunto A qualquer a relação de ser subconjunto próprio ($\subset$) é um ordem estrita sobre o conjunto $\wp(A)$.

Exemplo 4.13 Dado o conjunto $\{1, 2, 3\}$ a relação $\{(1, 2), (2, 3), (2, 2), (1, 3)\}$ não é uma ordem estrita pois $(2, 2)$ é um par pertencente a relação.

Definição 4.5 — Pré-ordem. Seja A um conjunto, uma relação $\sqsubseteq$ sobre A, é dita ser uma relação de pré-ordem sempre que $\sqsubseteq$ for reflexiva e transitiva.

Exemplo 4.14 Dado o conjunto $\{a, b, c\}$ a relação $\{(a, a), (b, b), (c, c), (b, c), (c, a), (b, a)\}$ é uma relação de pré-ordem.

Exemplo 4.15 A relação $\{(x, y) \in \mathbb{N}^2 \mid (\exists k \in \mathbb{N})[y = xk]\}$ é uma pré-ordem.

Exemplo 4.16 A relação $\{(x, y) \in \mathbb{N}^2 \mid x + y \neq x \text{ e } x + y \neq y\}$ não é uma pré-ordem pois não é reflexiva, basta notar que $(0, 0)$ não pertence a tal relação.

Aumentando as restrições sobre uma pré-ordem, isto é, adicionando mais propriedades a serem exigidas, é construída a noção de ordem parcial, tal conceito é formalizado a seguir.

Definição 4.6 — Ordem Parcial. Seja A um conjunto, uma relação $\sqsubseteq$ sobre A, é dita ser uma relação de ordem parcial sempre que $\sqsubseteq$ for reflexiva, antissimétrica e transitiva.

Como dito em [1] se $\sqsubseteq$ é uma ordem parcial sobre um conjunto A, então tem-se que $\sqsubseteq$ organizar (ou ordena) o conjunto A em uma determinada hierarquia (ou ordem), obviamente um mesmo conjunto pode apresentar diferentes ordenações, ou seja, podem existir diversas ordens parciais sobre A.

Tomando Notas 4.2 – A semântica das ordens! De forma geral quando $x \sqsubseteq y$ pode ser interpretado como x é anterior ou igual a y, entretanto, para o caso especifico das relações de ordem parcial $\leq$ e $\subseteq$ suas semânticas sãos as aquelas que o leitor já conhece, isto é, $x \leq y$ significa x é menor ou igual a y e $X \subseteq Y$ significa que X é subconjunto de Y.

Além das duas famosas ordens parciais mencionadas na Observação 4.2 a seguir serão apresentados mais algumas ordens parciais.

Exemplo 4.17 As seguintes relações são exemplos de ordens parciais:

(a) $\{(x, y) \in \mathbb{N}^2 \mid (\exists k \in \mathbb{N})[y = x + k]\}$.

(b) $\{(x, y) \in \mathbb{N}^2 \mid (\exists k \in \mathbb{N})[y = xk]\}$.

(c) Dado um conjunto A de todas as pessoas da terra a relação $x \; R \; y$ se, e somente se, x tem a mesma altura ou é mais alto que y, é uma ordem parcial sobre A.

Tomando Notas 4.3 – Sobre relação hierárquica entre os tipos de ordem! Fique atento e note que a ordem no item (b) do Exemplo 4.17 foi anteriormente usado como exemplo de uma pré-ordem, isso ocorre por que toda ordem parcial é uma pré-ordem.

Exemplo 4.18 Seja $A = \{a, b, c, d\}$ um conjunto a relação R definida como sendo

$$\{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c), (a, d)\}$$

é uma ordem parcial sobre A.

Exemplo 4.19 Dado $\{0, 1\}$ e a relação $\{(0, 0), (0, 1), (1, 1)\}$ é uma ordem parcial.

Exemplo 4.20 Dado um conjunto $\{0, 1, 2, 3\}$ a relação $\{(0, 0), (0, 1), (2, 2), (1, 2), (0, 2), (3, 3)\}$ não é uma ordem parcial pois o par $(1, 1)$ não pertence a relação e por definição uma ordem parcial deve ser reflexiva.

A partir da ideia de ordem parcial é possível definir o conceito de comparabilidade como se segue.

Definição 4.7 — Comparabilidade. Seja A um conjunto não vazio, $\sqsubseteq$ uma ordem parcial sobre A e seja $x, y \in A$, é dito que x e y são comparáveis sempre que $x \sqsubseteq y$ ou $y \sqsubseteq x$.

Como dito em [1, 14] tem-se que a noção de comparabilidade está ligada a ordem em questão, assim pode haver um conjunto A e uma ordem parcial $\sqsubseteq_1$ tal que dois elementos x e y são comparáveis, entretanto, pode haver outra ordem parcial $\sqsubseteq_2$ sobre o mesmo conjunto tal que os elementos x e y não pode ser comparáveis[2].

Exemplo 4.21 Considere o conjunto $A = \{1, 2, 3\}$ tem-se que $\subseteq$ será obviamente uma ordem parcial sobre $\wp(A)$, agora note que $\{1, 2\} \subseteq A$, portanto, $\{1, 2\}$ e A são comparáveis, por outro lado, $\{1, 2\} \not\subseteq \{1, 3\}$ e $\{1, 3\} \not\subseteq \{1, 2\}$, logo $\{1, 2\}$ e $\{1, 3\}$ são incomparáveis.

Exemplo 4.22 Dado o conjunto $\mathbb{R}$ e a ordem parcial $\leq$ sobre $\mathbb{R}$ tem-se que todo par de números reais (x, y) é sempre comparável.

Por fim é apresentado a ideia de ordem parcial, pela definição a seguir é fácil para o leitor perceber que toda ordem total é uma ordem parcial, porém, o oposto não é verdade.

Definição 4.8 — Ordem total. Uma ordem parcial $\sqsubseteq$ sobre um conjunto A é dita ser total quando para todo par de elementos $x, y \in A$ é comparável.

Exemplo 4.23 São exemplos de ordem totais:

(a) A ordem usual “menor igual” ($\leq$) sobre o conjunto $\mathbb{R}$.

(b) A relação $\{(a_0, a_0), (a_0, a_1), (a_0, a_2), (a_1, a_1), (a_1, a_2), (a_2, a_2)\}$ sobre o conjunto $\{a_0, a_1, a_2\}$.

Nesta seção ao apresentar a ideia de relações de ordem isso era feito pelo estudo da relação em si ficando seu conjunto base em segundo plano e com pouco interesse, agora serão considerados simultaneamente os dois conceitos juntos, ou seja, será agora apresentado o conceito de conjunto parcialmente ordenado.

4.4 *Posets* e Diagramas de Hasse

Como dito em [59], os conjuntos parcialmente ordenados ou *posets* (em inglês) têm uma longa história que remonta ao início do século XIX, onde as propriedades da ordenação dos subconjuntos de um conjunto foram investigadas. Embora o

[2]Em algumas obras é usado a escrita $x \not\sqsubseteq y$ para esboçar que x e y são incomparáveis por uma ordem parcial $\sqsubseteq$.

matemático Felix Hausdorff[3] (1868-1942) não tenha sido a pessoa que introduziu a ideia de conjunto parcialmente ordenado, foi ele que fez o primeiro estudo sério de uma teoria geral dos posets em seu trabalho [32].

Definição 4.9 — Poset. Um conjunto parcialmente ordenado ou *poset* é uma estrutura $\langle A, \sqsubseteq \rangle$ onde A é um conjunto não vazio e $\sqsubseteq$ é uma ordem parcial sobre A.

Exemplo 4.24 São exemplos de conjuntos parcialmente ordenados:

(a) $\langle \wp(A), \subseteq \rangle$.

(b) $\langle C, : \rangle$ onde $C = \{1, 2, 3, 4, 5, 6, 12\}$ e $x : y$ se, e somente se, x é um divisor de y.

(c) $\langle \mathbb{Z}, \geq \rangle$.

(d) $\langle B, \subseteq \rangle$ onde $B = \{R_1, R_2, \cdots\}$ é o conjunto de todas as relações binárias sobre um conjunto A.

Agora como dito em [55], muitas vezes é conveniente utilizar uma representação gráfica para os *posets* que possa evidenciar as relações hierárquicas existentes entre os elementos do conjunto base. Essa representação como dito em [1], é chamada de diagrama de Haase[4]. Vale salientar que tal representação não é para qualquer *poset* apenas os *posets* finitos podem ser representados por tais diagramas de forma completa.

O diagrama de Hasse é um grafo orientado acíclico construído utilizando a relação "x cobre y" sempre que $x \sqsubseteq y$, o diagrama é construído para um *poset* $\langle A, \sqsubseteq \rangle$ com A finito usando as seguintes regras:

(r_1) Para todo $x, y \in A$ se $x \sqsubseteq y$ e não existe um z tal que $x \sqsubseteq z$ e $z \sqsubseteq y$ com $x \neq y$, então o ponto de x aparece inferior no diagrama ao ponto de y.

(r_2) Para todo $x, y \in A$ se x e y satisfazem (r_1), então os pontos de x e y são ligados por segmento de reta.

(r_3) Todos os elementos $x \in A$ devem aparecer no diagrama como um ponto (ou nó).

Para ilustrar a construção de um diagrama de Hasse, considere o *poset* com a seguinte estrutura $\langle \{a, 2, 1, b\}, R \rangle$ onde $R = \{(1,1), (a,a), (1,a), (b,b), (1,b), (2,2), (b,2), (a,2), (1,2)\}$. Agora note que como $(1, a)$ satisfaz a regra (r_1), assim o ponto de 1 aparece inferior no diagrama ao ponto de a e o mesmo iriá valer para os casos $(1, b)$, $(a, 2)$ e $(b, 2)$, além disso, note que o 2 aparece relacionado sempre do lado direto da relação com todos os outros elementos do conjunto, logo pode-se estabelecer a seguinte distribuição espacial vista na Figura 4.1.

[3] Famoso por seus trabalhos em topologia.

[4] Em homenagem ao matemático alemão Helmut Hasse (1898-1979) que introduziu tais diagramas.

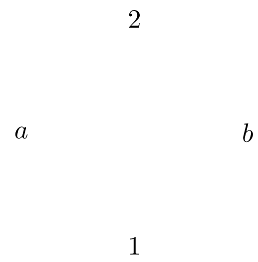


Figura 4.1: Distribuição espacial dos pontos para o diagrama de Hasse do *poset* $\langle\{a, 2, 1, b\}, R\rangle$.

Seguindo o desenvolver do diagrama, pode-se executando a regra (r_2) ligar todos os pontos no diagrama, afim de, ilustrar as relações entre os elementos, ficando o diagrama na forma apresentada a seguir:

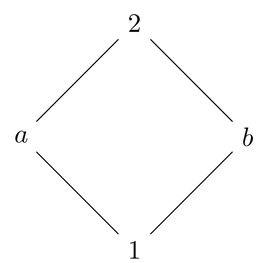


Figura 4.2: Diagrama de Hasse do *poset* $\langle\{a, 2, 1, b\}, R\rangle$.

Como todos os elementos de $\{a, 2, 1, b\}$ já estão no diagrama então não há nada mais a fazer.

Exemplo 4.25 O *poset* $\langle\{0, 1, c, d\}, Lip\rangle$ onde $Lip = \{(x, y) \mid x \leq y$ ou $(x \in \{0, 1\}, y \in \{a, b\})\}$ pode ser representado pelo diagrama a seguir.

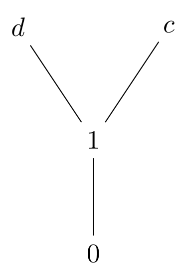
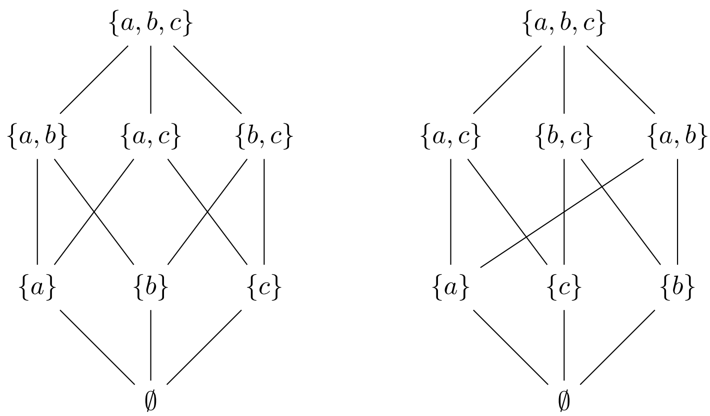


Figura 4.3: Diagrama de Hasse do *poset* $\langle\{0, 1, c, d\}, Lip\rangle$

Observação 4.1 — Sobre desenhar e representar! ALiCIA chama sua atenção para o fato que a representação por diagrama de Hasse não é única, em termos de distribuição espacial (desenho do grafo).

Exemplo 4.26 O *poset* $\langle \wp(\{a,b,c\}), \subseteq \rangle$ pode ser representado pelo dois diagramas a seguir.



(a) Representação em forma de cubo.

(b) Representação em forma de quase cubo.

Figura 4.4: Diagramas de Hasse para o *poset* $\langle \wp(\{a,b,c\}), \subseteq \rangle$.

Exemplo 4.27 O *poset* $\langle \{5,6,7,8,9\}, \leq \rangle$ é representado pelo diagrama a seguir.

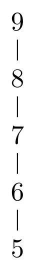


Figura 4.5: Diagrama de Hasse do *poset* $\langle \{5,6,7,8,9\}, \leq \rangle$

Posets cuja ordem é total também são chamados de cadeias (ver [1, 55]) e nesse caso o diagrama será uma linha reta com todos os elementos sobre essa linha, exatamente como no Exemplo 4.27. O leitor sem saber já usava esse conceito em seus estudo matemáticos a proferir frases como “a reta real” ou “a reta dos números reais”. Agora obviamente dado um diagrama de Hasse sempre é possível recuperar a estrutura do *poset* do mesmo, isto é, recuperar o conjunto base e a relação de ordem parcial que define o *poset*, a seguir são apresentados alguns exemplos disto.

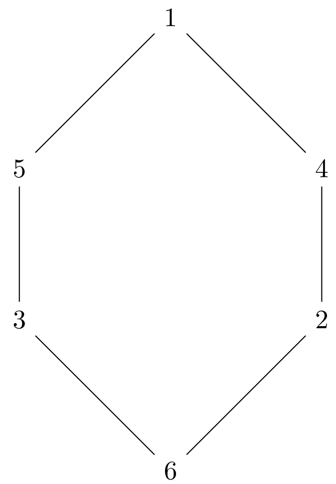


Figura 4.6: Um diagrama de Hasse.

Exemplo 4.28 Dado o diagrama de Hasse da Figura 4.6 a seguir, dado que 6 está ligado e abaixo de 3 e 2 tem-se que $(6,3),(6,2) \in R$ onde R é uma relação, o mesmo vale para os pares $(3,5),(2,4),(5,1)$ e $(4,1)$. Desse modo tal figura representa o *poset* $\langle A, R\rangle$ em que $A = \{1,2,3,4,5,6\}$ e R corresponde a relação $\{(6,3),(6,2),(3,5),(2,4),(5,1),(4,1),(6,5),(6,4),(6,1),(2,1),(5,1)\} \cup Id_A$.

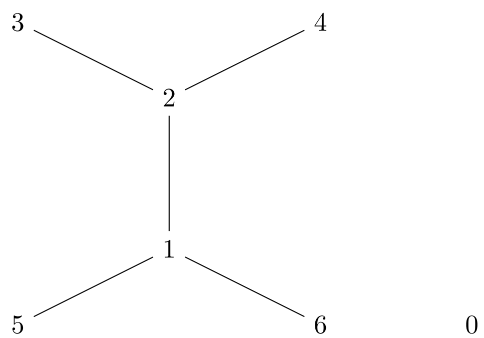


Figura 4.7: Um diagrama de Hasse.

Exemplo 4.29 Dado o diagrama de Hasse da Figura 4.7 representa o *poset* $\langle B, R_B\rangle$ em que: $B = \{0, 1, 2, 3, 4, 5, 6\}$ e

$$R_B = Id_B \cup \{(5,1),(6,1),(1,2),(2,3),(2,4)\} \cup \{(5,1),(6,1),(1,2),(2,3),(2,4)\}^+$$

Como dito em [14] um *poset* é uma álgebra relacional ordenado, ou ainda, uma álgebra[5] relacional[6], e como uma álgebra pode-se estudar: os elementos destacados, suas sub-álgebras (sub-estruturas) ou ainda os mecanismo de extensão da mesma. Na próxima seção este manuscrito irá realizar um estudo sobre os pontos.

4.5 Elementos Notáveis de um *Poset*

Como muito bem aprofundado em [14, 55, 59], existem diverso conceitos e aplicações interessantes ligados a ideia de *posets*, assim para ajudar que leitor tenha uma formação sólida na área de teoria dos *posets* é interessante apresentar alguns deste conceitos chaves da teoria, neste seção serão trabalhos os elementos notáveis existes nos *posets* e suas propriedades.

Definição 4.10 — Máximo e Mínimo de um subconjunto. Seja $\langle A, \sqsubseteq\rangle$ um *poset* e $X \subseteq A$ o máximo de X, denotado por $max(X)$, é um elemento $x \in X$ tal que para todo $y \in X$ tem-se que $y \sqsubseteq x$. O mínimo de X, denotado por $min(X)$, é um elemento $x \in X$ tal que para todo $y \in X$ tem-se que $x \sqsubseteq y$.

Exemplo 4.30 Considere o *poset* da Figura 4.2 para o conjunto $X = \{1, 2, a\}$ tem-se que $min(X) = 1$ e $max(X) = 2$.

Exemplo 4.31 Considere o *poset* da Figura 4.3 para o conjunto $X = \{0, 1\}$ tem-se que $min(X) = 0$ e $max(X) = 1$.

Exemplo 4.32 Considere o *poset* da Figura 4.4a para o conjunto $X = \{\{a, b\}, \{a\}, \{b\}, \emptyset\}$ tem-se que $min(X) = \emptyset$ e $max(X) = \{a, b\}$.

Agora é conveniente ressaltar que tanto máximo quando o mínimo podem vir há não existir, isto é, dado um *poset* $\langle A, \sqsubseteq\rangle$ um subconjunto X de A pode-se de tal forma que ele não contenha máximo e(ou) mínimo.

Exemplo 4.33 Considere o *poset* ilustrado pela Figura 4.6 o subconjunto $\{3, 2, 5, 4\}$ deste *poset* não apresenta máximo e nem mínimo.

[5] O conceito de álgebra será melhor formalizado em capítulos futuros deste manuscrito, por hora o leitor pode pensar em uma álgebra como uma estrutura.

[6] Uma álgebra relacional é uma estrutura criada na interseção da lógica de primeira ordem e da álgebra booleana (ou álgebra de conjuntos) finita, tal tipo de álgebra é de suma importância para a área de banco de dados.

Exemplo 4.34 Considere o *poset* ilustrado pela Figura 4.7 o subconjunto $\{1, 5, 6\}$ deste *poset* possui máximo mas não possui mínimo.

Teorema 4.4 — Unicidade do máximo. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Se existe $x \in X$ tal que $max(X) = x$, então x é único.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Suponha por absurdo que existem $x, x' \in X$ tal que $max(X) = x$ e $max(X) = x'$ com $x \neq x'$, logo por definição para todo $a \in X$ tem-se que $a \sqsubseteq x$ e $a \sqsubseteq x'$, mas desde que $x, x' \in X$ tem-se que $x \sqsubseteq x'$ e $x' \sqsubseteq x$ e, desde que, $\sqsubseteq$ é antissimétrica tem-se que $x = x'$ o que contradiz a hipótese e, portanto, se existe o máximo de X ele é único. □

Teorema 4.5 — Unicidade do mínimo. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Se existe $x \in X$ tal que $min(X) = x$, então x é único.

Demonstração. Similar a demonstração do Teorema 4.4. □

Teorema 4.6 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$ com $X \subseteq Y$ tem-se que:

(i) Se $max(X) = a$ e $max(Y) = b$, então $a \sqsubseteq b$.

(ii) Se $min(X) = a$ e $min(Y) = b$, então $b \sqsubseteq a$.

Demonstração. A demonstração é simples e fica como exercício ao leitor. □

Além da ideia de máximo e mínimo sobre os *posets* também definido a ideia de maximais e minimais.

Definição 4.11 — Elementos maximais. Seja $\langle A, \sqsubseteq \rangle$ um *poset* um elemento $x \in A$ é dito ser um maximal se para todo $y \in A$ tem-se que se $x \sqsubseteq y$, então $x = y$.

Exemplo 4.35 Considere o *poset* esboçado pela Figura 4.8 a seguir. Para tal *poset* tem-se que o elemento g é um maximal e também é o máximo do conjunto.

Exemplo 4.36 Considere o *poset* esboçado pela Figura 4.6. Para tal *poset* tem-se que o elemento 1 é um maximal e também é o máximo do conjunto.

Em algumas situações elementos maximais coincidem com o máximo, entretanto, como mostrado a seguir ser maximal não é garantia de ser o máximo do conjunto.

Exemplo 4.37 Considere o *poset* esboçado pela Figura 4.9 a seguir. Para tal *poset* tem-se que os elementos 4 e 5 satisfazem a Definição 4.11 logo ambos são maximais do conjunto, porém, ambos são incomparáveis, portanto, nenhum é o máximo do conjunto.

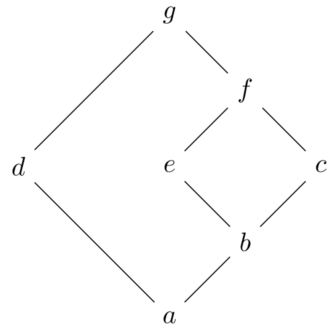


Figura 4.8: Um *poset* representado por um diagrama de Hasse.

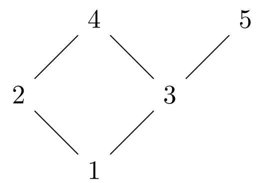


Figura 4.9: Um *poset* representado por um diagrama de Hasse.

De forma dual ao conceito de maximal pode-se definir a ideia de elemento minimal, e isto é feito como se segue.

Definição 4.12 — Elementos minimais. Seja $\langle A, \sqsubseteq \rangle$ um *poset* um elemento $x \in A$ é dito ser um minimal se para todo $y \in A$ tem-se que se $y \sqsubseteq x$, então $x = y$.

Exemplo 4.38 Considerando o *poset* da Figura 4.8 tem-se que o elemento a é minimal de tal conjunto e também apresenta a característica de ser o mínimo.

Exemplo 4.39 Considerando o *poset* da Figura 4.9 tem-se que o elemento 1 é minimal de tal conjunto e também apresenta a característica de ser o mínimo.

Exemplo 4.40 Considerando o *poset* da Figura 4.7 tem-se que os elementos 5 e 6 são ambos minimais, porém, como são ambos incomparáveis tem-se que nenhum dos dois é o mínimo do conjunto base do *poset*.

Exemplo 4.41 Considere o *poset* da Figura 4.10 a seguir, tem-se que g e f são elementos maximais e c, a e b são elementos minimais, note que tal *poset* não possui máximo e mínimo.

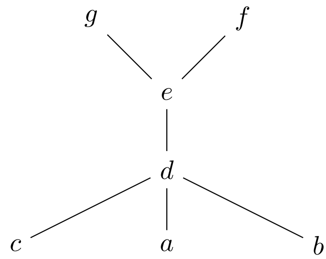


Figura 4.10: Um *poset* representado por um diagrama de Hasse.

Definição 4.13 — Majorante. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$, um elemento $x \in A$ é dito ser um majorante (ou cota superior) de X sempre que para todo $y \in X$ tem-se que $y \sqsubseteq x$.

Exemplo 4.42 Considere o *poset* esboçado na Figura 4.10 e o subconjunto $X = \{e, d, c\}$ tem-se que os elementos e, f e g são todos majorantes de X. Já os subconjuntos $Y = \{g, f, e\}$ e $Z = \{g, f, a\}$ não possuem majorantes.

Exemplo 4.43 Considere o *poset* esboçado na Figura 4.9 e o subconjunto $X = \{2, 3, 5\}$ não possui majorantes, já o conjunto $Y = \{1, 2, 3, 4\}$ possui o elemento 4 como majorante.

Exemplo 4.44 Considere o *poset* esboçado na Figura 4.8 e o subconjunto $X = \{d, e, f\}$ tem-se que o elemento g é o majorante de X.

Como mencionado em [1] se x é um majorante (ou cota superior) de um conjunto X, é dito que X é um conjunto majorado pelo elemento x ou que o conjunto X possui uma cota superior x.

Definição 4.14 — Conjunto dos majorantes. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$, o conjunto de todos os majorantes de X é denotado por $X_{\uparrow}$.

Como dito em [1, 14, 55] a maior parte dos conceito na teoria dos *posets* tem natureza dual, assim é natural que seja imediatamente apresentadas as definições de minorantes e conjunto dos minorantes.

Definição 4.15 — Minorante. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$, um elemento $x \in A$ é dito ser um minorante (ou cota inferior) de X sempre que para todo $y \in X$ tem-se que $x \sqsubseteq y$.

Exemplo 4.45 Considere o *poset* esboçado na Figura 4.10 e o subconjunto $X = \{e, d, c\}$ tem-se que o elemento c é o minorante de X. Já os subconjuntos $Y = \{g, f, e\}$ tem como minorantes os elementos e, d, c, ae b, por fim, para o conjunto $Z = \{g, f, a\}$ o único minorantes é o elemento a.

Exemplo 4.46 Considere o *poset* esboçado na Figura 4.9 e o subconjunto $X = \{2, 3, 5\}$ tem como minorante o elemento 1, já o conjunto $Y = \{3, 4, 5\}$ possui como minorantes os elementos 1 e 3.

Exemplo 4.47 Considere o *poset* esboçado na Figura 4.8 e o subconjunto $X = \{d, e, f\}$ tem-se que o elemento a é o único minorante deste conjunto, já para o conjunto $Y = \{g, f\}$ tem-se os elementos f, e, c, b e a como minorantes de Y.

Definição 4.16 — Conjunto dos minorantes. Seja $\langle A, \sqsubseteq\rangle$ um *poset* e $X \subseteq A$, o conjunto de todos os minorantes de X é denotado por $X_{\downarrow}$.

Teorema 4.7 Seja $\langle A, \sqsubseteq\rangle$ um *poset* e $X \subset A$. Se $a \in A$ é um majorante (minorante) de X e $a \in X$, então $a = max(X)$ $(a = min(X))$.

Demonstração. Trivial. □

O próximo resultado estabelece que o conjunto de majorantes e minorantes respeita a monotonicidade da relação inclusão.

Teorema 4.8 Seja $\langle A, \sqsubseteq\rangle$ um *poset* e $X, Y \subseteq A$. Se $X \subseteq Y$, então:

(i) $Y_{\uparrow} \subseteq X_{\uparrow}$.

(ii) $Y_{\downarrow} \subseteq X_{\downarrow}$.

Demonstração. A demonstração é simples e ficará como exercício ao leitor. □

Definição 4.17 — Conjunto limitado. Seja $\langle A, \sqsubseteq\rangle$ um *poset* e $X \subseteq A$, o conjunto X é dito ser limitado em A sempre que X possui majorantes e minorantes.

Exemplo 4.48 Considere o *poset* $\langle \mathbb{N}, \leq\rangle$ o conjunto $X_{k_1,k_2} = \{x \in \mathbb{N} \mid k_1 < x < k_2\}$ é um conjunto que sempre possuirá majorantes e minorantes (a saber k_1 e k_2) logo ele é um conjunto limitado em $\langle \mathbb{N}, \leq\rangle$.

Exemplo 4.49 Considere o *poset* $\langle \wp(A), \subseteq \rangle$ onde A é um conjunto qualquer, um conjunto $X \in \wp(A)$ sempre irá possuir minorante e majorante, que como dito em [1] são gerados pela interseção e união respectivamente. Assim qualquer $X \in \wp(A)$ sempre será um conjunto limitado em $\langle \wp(A), \subseteq \rangle$.

Exemplo 4.50 Considere o *poset* esboçado na Figura 4.10 e o subconjunto $X = \{e, d, c, a, b\}$ tem-se que tal conjunto possui os majorantes e, g e f, mas não possui minorantes, assim X não é limitado.

Teorema 4.9 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Se $X \neq \emptyset$, então $X \subseteq (X_{\downarrow})_{\uparrow}$.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$, suponha que $X \neq \emptyset$, assim para todo $x \in X$ e cada $y \in X_{\downarrow}$ tem-se que $y \sqsubseteq x$, logo $x \in (X_{\downarrow})_{\uparrow}$, portanto, $X \subseteq (X_{\downarrow})_{\uparrow}$. □

Teorema 4.10 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Se $X \neq \emptyset$, então $X \subseteq (X_{\uparrow})_{\downarrow}$.

Demonstração. Similar a prova do Teorema 4.9. □

Teorema 4.11 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Se $X \neq \emptyset$, então:

(i) $X_{\uparrow} = ((X_{\uparrow})_{\downarrow})_{\uparrow}$.

(ii) $X \downarrow = ((X_{\downarrow})_{\uparrow})_{\downarrow}$.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Suponha que $X \neq \emptyset$, assim tem-se que:

(i) Pelo Teorema 4.10 segue que $X_{\uparrow} \subseteq ((X_{\downarrow})_{\uparrow})_{\downarrow}$, por outro lado, pelo Teorema 4.9 pode-se concluir que $((X_{\uparrow})_{\downarrow})_{\uparrow} \subseteq X_{\uparrow}$, portanto, pela Definição 1.6 tem-se que $X_{\uparrow} = ((X_{\uparrow})_{\downarrow})_{\uparrow}$.

(ii) Similar ao item anterior.

Completando assim a prova. □

Teorema 4.12 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$. Se $X, Y \neq \emptyset$, então:

(i) $(X \cup Y)_{\downarrow} = X_{\downarrow} \cap Y_{\downarrow}$.

(ii) $(X \cup Y)_{\uparrow} = X_{\uparrow} \cap Y_{\uparrow}$.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$. Suponha que $X \neq \emptyset$, assim tem-se que:

(i) Desde que $X \subseteq X \cup Y$ e $Y \subseteq X \cup Y$ tem-se pelo Teorema 4.8 que $(X \cup Y)_{\downarrow} \subseteq X_{\downarrow}$ e $(X \cup Y)_{\downarrow} \subseteq Y_{\downarrow}$, consequentemente, $(X \cup Y)_{\downarrow} \subseteq X_{\downarrow} \cap Y_{\downarrow}$. Por outro lado, para todo $x \in X_{\downarrow} \cap Y_{\downarrow}$ tem-se para todo $y \in X$ que $x \leq y$ e para todo $z \in Y$ que $x \leq z$, assim $x \in (X \cup Y)_{\downarrow}$ e assim $(X \cup Y)_{\downarrow} \subseteq X_{\downarrow} \cap Y_{\downarrow}$ e, portanto, pela Definição 1.6 tem-se que $(X \cup Y)_{\downarrow} = X_{\downarrow} \cap Y_{\downarrow}$.

(ii) Similar ao item anterior.

O que termina a prova. □

Definição 4.18 — Supremo. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$ o supremo de X (caso exista), denotado por $sup(X)$, é o menor dos majorantes, em notação formal tem-se que $sup(X) = min(X_{\uparrow})$.

Como dito em [1, 14], uma forma de caracterização do supremo é através de suas propriedades inerentes, e isto é feito da seguinte forma, dado um *poset* $\langle A, \sqsubseteq \rangle$ tem-se que $sup(X) = a$ se, e somente se:

1. $a \in A$.
2. Para todo $x \in X$ tem-se que $x \sqsubseteq a$.
3. Se $a' \in A$ e para todo $x \in X$ tem-se que $x \sqsubseteq a'$, então $a \sqsubseteq a'$.

Note que a propriedade (1) diz que o supremo (caso exista) é sempre um elemento do poset, já a propriedade (2) estabelece que o supremo deve ser um majorante e a propriedade (3) estabelece que o supremo deve ser a menor cota superior, isto é, o mínimo do conjunto dos majorantes.

Definição 4.19 — Ínfimo. Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X \subseteq A$ o ínfimo de X (caso exista), denotado por $inf(X)$, é o maior dos minorantes, em notação formal tem-se que $sup(X) = max(X_{\downarrow})$.

Dualmente ao supremo como dito em [1, 14], uma forma de caracterização do ínfimo é através de suas propriedades inerentes, e isto é feito da seguinte forma, dado um *poset* $\langle A, \sqsubseteq \rangle$ tem-se que $inf(X) = a$ se, e somente se:

1. $a \in A$.
2. Para todo $x \in X$ tem-se que $a \sqsubseteq x$.
3. Se $a' \in A$ e para todo $x \in X$ tem-se que $a' \sqsubseteq x$, então $a' \sqsubseteq a$.

Ou seja, a propriedade (1) diz que o ínfimo (caso exista) é sempre um elemento do poset, já a propriedade (2) estabelece que o ínfimo deve ser um minorante e a propriedade (3) estabelece que o ínfimo deve ser a maior cota inferior, isto é, o máximo do conjunto dos minorantes.

Tomando Notas 4.4 – Sobre nomenclatura! ALiCIA aprendeu, lendo [14] e [71], que os termos *least upper bound* (menor cota superior) e *join* são sinônimos de supremo, enquanto, que *greatest lower bound* (maior cota inferior) e *meet* são sinônimos de ínfimo.

Exemplo 4.51 Considere o *poset* representado pela Figura 4.11 a seguir, o subconjunto $X = \{2, 3, 4, 5\}$ é tal que $sup(X) = 7$ e $inf(X) = 2$, por lado, para o subconjunto $Y = \{1, 0, 2, 4\}$ tem-se que $sup(Y) = 3$ mas não existe um ínfimo de tal conjunto. Além disso, pegando o conjunto inteiro do *poset* tem-se que o conjunto possui supremo, a saber 7 mas não possui ínfimo.

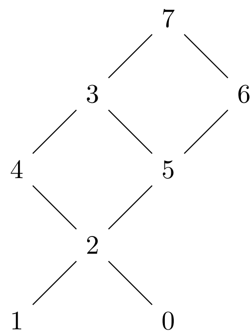


Figura 4.11: Diagrama de Hasse do *poset* do Exemplo 4.51.

Exemplo 4.52 Considerando o *poset* $\langle \mathbb{Q}, \leq \rangle$ tem-se que o subconjunto $\{x \in \mathbb{Q} \mid x^2 \leq 2\}$ não possui supremo pois $\sqrt{2} \notin \mathbb{Q}$.

Teorema 4.13 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$. Se $X \subseteq Y$ e além disso X e Y possuem supremo, então $sup(X) \sqsubseteq sup(Y)$.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$, assuma $X \subseteq Y$ e que que X e Y possuem supremo, assim pelo Teorema 4.8(i) tem-se que $Y_\uparrow \subseteq X_\uparrow$. Mas pelo Teorema 4.6(ii) tem-se que $min(Y_\uparrow) \sqsubseteq min(X_\uparrow)$, logo $sup(X) \sqsubseteq sup(Y)$. □

Teorema 4.14 Seja $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$. Se $X \subseteq Y$ e além disso X e Y possuem ínfimo, então $inf(Y) \sqsubseteq inf(X)$.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset* e $X, Y \subseteq A$, assuma $X \subseteq Y$ e que que X e

Y possuem supremo, assim pelo Teorema 4.8(ii) tem-se que $Y_\uparrow \subseteq X_\uparrow$. Mas pelo Teorema 4.6(i) tem-se que $max(Y_\downarrow) \sqsubseteq max(X_\downarrow)$, logo $inf(Y) \sqsubseteq inf(X)$. □

Teorema 4.15 Se $\langle A, \sqsubseteq \rangle$ é um *poset*, $X \subseteq A$ com $sup(X_\downarrow) = a$ e $a \in A$, então $inf(X) = sup(X_\downarrow)$.

Demonstração. $\langle A, \sqsubseteq \rangle$ é um *poset*, $X \subseteq A$ com $sup(X_\downarrow) = a$ e $a \in A$, agora note que para qualquer que seja $x \in X$ e $y \in X_\downarrow$ tem-se que $y \sqsubseteq x$, e assim x é claramente um majorante de $X_\downarrow$, ou seja, $x \in (X_\downarrow)_\uparrow$, consequentemente, $a \sqsubseteq y$, uma vez que, $sup(X_\downarrow) = a$, assim a é um minorante de X, ou seja, $a \in X_\downarrow$. Por outro lado, para qualquer $z \in X_\downarrow$ tem-se que $z \sqsubseteq a$ e, portanto, $a = inf(X)$. □

Teorema 4.16 Se $\langle A, \sqsubseteq \rangle$ é um *poset*, $X \subseteq A$ com $inf(X_\downarrow) = a$ e $a \in A$, então $sup(X) = inf(X_\uparrow)$.

Demonstração. Similar a demonstração do Teorema 4.15. □

Quando um conjunto X satisfaz o Teorema 4.15 é dito que ele é inferiormente limitado, e quando ele satisfaz o Teorema 4.16 é dito que ele é superiormente limitado. Quando ele satisfaz os dois então ele satisfaz a Definição 4.17.

Teorema 4.17 Se $\langle A, \sqsubseteq \rangle$ é um *poset*, então as seguintes asserções são equivalentes:

(1) Todo subconjunto não vazio superiormente limitado de A possui supremo.

(2) Todo subconjunto não vazio inferiormente limitado de A possui ínfimo.

Demonstração. Dado $\langle A, \sqsubseteq \rangle$ um *poset*, tem-se que:

(1) $\Rightarrow$ (2) Assuma que todo subconjunto não vazio superiormente limitado de A possui supremo, agora seja $X \subseteq A$ limitado inferiormente, ou seja, $X_\downarrow \neq \emptyset$, agora obviamente cada $x \in X$ é tal que x é um majorante de $X_\downarrow$, ou seja, $x \in (X_\downarrow)_\uparrow$ e, portanto, $X_\downarrow$ é superiormente limitado, logo pelo Teorema 4.16 existe o supremo do conjunto $X_\downarrow$, consequentemente pelo Teorema 4.15 existe o ínfimo de $X_\downarrow$.

(2) $\Rightarrow$ (1) Similar ao item anterior. □

4.6 Boa Ordenação e Relações Bem Fundadas

Agora que o leitor chegou até este ponto significa que está pronto para a apresentação ligada a ideia de boas ordens e ordem bem fundadas.

Definição 4.20 — Boa ordem. Uma ordem parcial $\sqsubseteq$ sobre um conjunto A é dita uma boa ordem sempre que para todo subconjunto não vazio B de A é tal que B possui elemento mínimo com respeito a ordem $\sqsubseteq$.

O leitor mais atento pode ter notado que Definição 4.20 oculta o fato de que uma boa ordem é necessariamente um ordem total. Como dito em [48], sempre que $\sqsubseteq$ for uma boa ordem a estrutura $\langle A, \sqsubseteq \rangle$ será chamada de conjunto bem ordenado.

Exemplo 4.53 A relação $\leq$ é uma boa ordem com respeito ao conjunto dos números naturais, entretanto, se considerada sobre o conjuntos dos números inteiros ou reais ele não se classifica mais como uma boa ordem.

Teorema 4.18 Uma estrutura $\langle A, \sqsubseteq \rangle$ é um conjunto bem ordenado se, e somente se, todo subconjunto não vazio de A possui elemento mínimo.

Demonstração. ($\Rightarrow$) A ida é trivial pela própria Definição 4.20. ($\Leftarrow$) Assuma que todo subconjunto não vazio de A possui elemento mínimo, assim existe $z = min(A)$ e além disso tem-se que, dado $x, y \in A$ tem-se que $\{x, y\}$ tem menor elemento, ou seja, uma das três possibilidades acontece, $x \sqsubset y, y \sqsubset x$ ou $y = x$, entretanto, isso implica que qualquer dois elementos de A são comparáveis e, portanto, $\sqsubseteq$ é um ordem total é assim $\langle A, \sqsubseteq \rangle$ é um conjunto bem ordenado. $\square$

Note que a volta na demonstração do Teorema 4.18 estabelece que uma ordem ser total é uma condição necessária para que ela seja uma boa ordem, por outro lado, o exemplo 4.53 mostra que nem toda ordem total é de fato uma boa ordem. A seguir é apresentado o princípio da boa ordenação, neste texto não será apresentado sua demonstração, entretanto, é interessante que o leitor saiba que tal princípio foi apresentado pelo grande matemático Ernst Zermelo[7] (1871-1953), e que tal princípio é equivalente ao axioma da escolha [14] (tratado em momentos futuros deste manuscrito).

Princípio 4.1 — Princípio da Boa Ordenação. Sobre qualquer conjunto A é possível definir uma boa ordem $\trianglelefteq$.

Pode-se agora apresentar um enfraquecimento da noção de boa ordem, que terá grande importância quando este manuscrito estiver tratado dos conceitos de indução, estruturas indutivamente geradas e recursão.

Definição 4.21 — Relação Bem Fundada. Uma relação binária R sobre um conjunto A é dita ser bem fundada, se não existem cadeias descendentes infinitas, em outras palavras, não existem elementos $a_0, a_1, a_2, \cdots \in A$ tal que, $\cdots \trianglelefteq a_n \trianglelefteq a_{n-1} \trianglelefteq \cdots \trianglelefteq a_2 \trianglelefteq a_1 \trianglelefteq a_0$.

Observe que Definição 4.21 estabelece que a cadeia relacional não pode crescer infinitamente na direção da esquerda da relação, e portanto, deve existir um elemento no conjunto que seria visto com ponto extremo esquerdo da relação. Além disso, ainda pela a Definição 4.21 é notável que uma relação bem fundada pode ser não é transitiva, considere por exemplo a relação sobre os naturais da forma $R = \{(x, y) \in \mathbb{N}^2 \mid y = x + 1\}$, ela atende claramente as condições para ser uma relação bem fundada, entretanto, perceba que ela não é transitiva pois obviamente $0 \; R \; 1, 1 \; R \; 2$ mas $0 \not R \; 2$, portanto, ela é bem fundada mas não é transitiva.

[7]Zermelo junto com Adolf Abraham Halevi Fraenkel (1891-1965) desenvolveu o sistema formal hoje conhecido como teoria axiomática dos conjuntos.

Exemplo 4.54 Dado o conjunto dos números naturais as relações $<$ e $\leq$ são respectivamente uma relação bem fundada e um uma relação que não é bem fundada.

Exemplo 4.55 Dado o conjunto dos números inteiros tem-se que a relação $<$ não é bem fundada.

Exemplo 4.56 Dado o conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ a relação $\subset$ é uma relação bem fundada sobre $\wp(A)$.

A seguir serão apresentados alguns resultados interessantes sobre as relação bem fundadas, em especial será apresentado uma forma de caracterização das relações bem fundadas.

Proposição 4.1 Se R é uma relação bem fundada em A, então R é irreflexiva.

Demonstração. Suponha por absurdo que R é uma relação bem fundada sobre um conjunto A e que R é reflexiva, logo para todo $a \in A$ tem-se que $a\ R\ a$ e, portanto, existe uma cadeia infinita da seguinte forma $\cdots\ R\ a\ R\ a\ R \cdots R\ a\ R\ a\ R\ a$ o que contradiz a hipótese de R seja uma relação bem fundada. Consequentemente, se R é uma relação bem fundada, então ela deve ser irreflexiva. $\square$

Teorema 4.19 — Teorema de Caracterização. Seja $\trianglelefteq$ uma relação binária sobre A. Tem-se que $\trianglelefteq$ é uma relação bem fundada se, e somente se, todo subconjunto não vazio X de A possui elemento minimal[a].

[a]O sentido de minimal aqui extrapola a ideia de minimal em respeito a ordem, visto que $\trianglelefteq$ não é necessariamente um ordem parcial, aqui o sentido de minimal é que: $x \in X$ e não existe um $a \in X$ com $a \trianglelefteq x$

Demonstração. ($\Rightarrow$) Suponha por absurdo que $\trianglelefteq$ é uma relação bem fundada e que existe um subconjunto não vazio X de A que não possui elemento minimal, assim sendo $X = \{a_1, a_2, \cdots\}$ tem-se que a_1 em X não é minimal, logo existe a_2 em X tal que $a_2 \trianglelefteq a_1$, mas como a_2 também não é minimal existe um a_3 tal que $a_3 \trianglelefteq a_2$ e assim sucessivamente, consequentemente, existindo uma cadeia infinita a esquerda da forma, $\cdots \trianglelefteq a_3 \trianglelefteq a_2 \trianglelefteq a_1$, mas isso contradiz a hipótese de $\trianglelefteq$ se uma relação bem fundada e, portanto, tem-se que se $\trianglelefteq$ é bem fundada, todo subconjunto não vazio X de A irá possuir (pelo menos um) elemento minimal. ($\Leftarrow$) Suponha por absurdo que $\trianglelefteq$ não é uma relação bem fundada e que todo subconjunto não vazio X de A possui elemento minimal (logo existe $x \in X$ e não existe um $a \in X$ com $a \trianglelefteq x$). Como $\trianglelefteq$ não é bem fundada pode-se assumir que exista uma cadeia infinita a esquerda $\cdots \trianglelefteq a_3 \trianglelefteq a_2 \trianglelefteq a_1$, agora deixe a_i ser o elemento minimal de X logo não pode existir um a_{i+1} tal que $a_{i+1} \trianglelefteq a_i$ o que contradiz a hipótese da existência da cadeia infinita, ou seja, contradiz a hipótese de $\trianglelefteq$ não ser bem fundada, consequentemente, pode-se afirma que, se todo subconjunto não vazio X de A possui elemento minimal, então $\trianglelefteq$ é uma relação bem fundada. $\square$

O próximo resultado revela ao leitor o estreito relacionamento entre a boa ordem e as relações bem fundadas, o resultado mostra que ser boa ordem é condição suficiente para ser uma relação bem fundado, porém ser bem fundada não é suficiente para ser uma boa ordem, ou seja, em um certo sentido as relação bem fundadas são mais exigentes.

Teorema 4.20 Seja $\langle A, \trianglelefteq \rangle$ uma álgebra relacional tem-se que:

(i) Se $\trianglelefteq$ é uma boa ordem, então $\trianglelefteq$ é uma relação bem fundada.

(ii) Se $\trianglelefteq$ é uma relação bem fundada e total[a], então $\trianglelefteq$ é uma boa ordem.

[a] A totalidade de uma relação bem fundada $\trianglelefteq$ está associado a ideia que quais $x, y \in A$ são comparáveis por $\trianglelefteq$.

Demonstração. Dado uma álgebra relacional $\langle A, \trianglelefteq \rangle$ tem-se que:

(i) Suponha que $\trianglelefteq$ é uma boa ordem, assim pela Definição 4.20 tem-se que todo subconjunto não vazio de A tem elemento mínimo, como todo elemento mínimo é também um minimal tem-se pelo Teorema 4.19 que $\trianglelefteq$ é uma relação bem fundada.

(ii) Assuma que $\trianglelefteq$ é uma relação bem fundada e total, logo tem-se que:

- Por $\trianglelefteq$ ser bem fundada pela Proposição 4.1 tem-se que R é irreflexiva.
- Agora pela totalidade de $\trianglelefteq$ tem-se para quaisquer $x, y, z \in A$ tais que $x \trianglelefteq y$ e $y \trianglelefteq z$ tem-se que $x = z$ iria implicar em uma cadeia infinita à esquerda, o que é impossível uma vez que $\trianglelefteq$ é uma relação bem fundada, por outro lado, se $z \trianglelefteq x$ fosse possível novamente seria possível construir uma cadeia infinita à esquerda o que novamente é um absurdo pelo fato de $\trianglelefteq$ ser bem fundada, logo tem-se que $x \trianglelefteq z$ e, portanto, $\trianglelefteq$ é transitiva.

Pelo fato de $\trianglelefteq$ ser transitiva, irreflexiva e total tem-se que R será uma ordem total estrita. Agora pelo Teorema 4.19 uma vez que $\trianglelefteq$ é bem fundada tem-se que todo subconjunto não vazio X de A possui elemento minimal x, entretanto, em um ordem total todo minimal é mínimo (provar isto fica como exercício), consequentemente, pela Definição 4.20 tem-se que $\trianglelefteq$ é uma boa ordem. $\square$

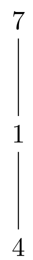
4.7 Operações Entre *Posets*, Novas Ordens e Ordem Lexicográfica

Como dito em [55], diversas operações podem ser definidas entre *posets*, além disso, é muito comum dado dois *posets* $\langle A, \sqsubseteq_A \rangle$ e $\langle B, \sqsubseteq_B \rangle$ buscar definir novas ordens parciais sobre os conjuntos $A \cup B$ e $A \times B$ usando como base as ordens pré-existentes $\sqsubseteq_A$ e $\sqsubseteq_B$. Nesta seção serão estudadas operações entre *posets* e também e como construir novas ordens parciais a partir de ordens parciais já existentes.

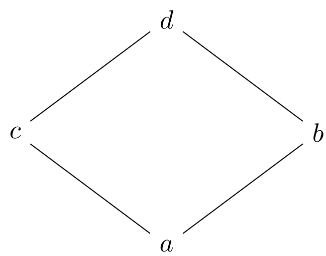
Definição 4.22 — Soma Cardinal. Dado dois *posets* $\langle A, \sqsubseteq_A \rangle$ e $\langle B, \sqsubseteq_B \rangle$ tal que $A \cap B = \emptyset$, a soma cardinal deste dois *posets*, denotado por $A \boxplus B$, consiste no *poset* $\langle A \cup B, \sqsubseteq_\boxplus \rangle$, onde $x \sqsubseteq_\boxplus y$ se, e somente se, $x \sqsubseteq_A y$ ou $x \sqsubseteq_B y$.

Apesar de não estar explicitamente escrito, note que, a Definição 4.22 estabelece que $x \sqsubseteq_\boxplus y$ acontece em apenas dois casos específicos, no primeiro caso ($x \sqsubseteq_A y$) tem -se $x, y \in A$, já no segundo caso ($x \sqsubseteq_B y$) obrigatoriamente $x, y \in B$, em qualquer outra situação os elementos x e y pertenceram a conjuntos distintos e nesse cenário eles serão incomparáveis, assim a relação $\sqsubseteq_\boxplus$ beira a trivialidade. Claramente o diagrama de Hasse para a ordem $\sqsubseteq_\boxplus$ é basicamente um diagrama em que os diagramas das ordens $\sqsubseteq_A$ e $\sqsubseteq_B$ são posto lado a lado, o exemplo a seguir ilustra esta ideia.

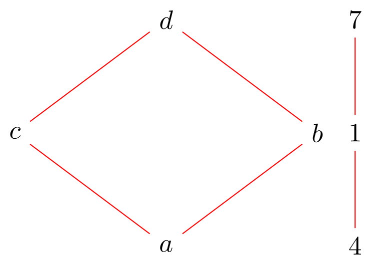
Exemplo 4.57 Considerando os conjuntos $A = \{1, 4, 7\}$ e $B = \{a, b, c, d\}$ ordenados respectivamente pelas ordens R_1 e R_2 descritas pelos diagramas 4.12a e 4.12b da Figura 4.12, e a soma cardinal de ambos os *posets* é representada pelo diagrama (destacado com linhas vermelhas) 4.12c da Figura 4.12.



(a) Poset $\langle A, R_1 \rangle$.



(b) Poset $\langle B, R_2 \rangle$.



(c) Soma cardinal $A \boxplus B$

Figura 4.12: Dois *Posets* e sua soma cardinal.

Terminar de escrever a seção de operações sobre *Poset* depois!!!!

4.8 Questionário

Questão 4.1 Seja B o conjunto de todos os brasileiros e R uma relação definida sobre B como $x \; R \; y$ se, e somente se, x e y são nascidos no mesmo estado ou território do Brasil. Responda as questões a seguir[8] e justifique sua resposta.

(a). Quantas classes de equivalência diferentes são determinadas por R?

(b). Escreva em notação compacta a classe de equivalência definida por Heitor Villa-Lobos.

(c). Responda se Getúlio Vargas $\in$ [Heitor Villa-Lobos].

(d). Responda se Luiz Gonzaga $\in$ [João Gilberto].

(e). Escreva em notação compacta a classe de equivalência definida por Leopoldo Nachbin.

(f). Responda se César Lattes $\notin$ [Mário Schenberg].

(g). Argumente sobre a seguinte asserção: se Mário Schenberg $\in$ [Leopoldo Nachbin], então Mário Schenberg $\in$ [José Leite Lopes].

Questão 4.2 Considerando o conjunto $A = \mathbb{N}^2$ demonstre que a relação

$$R = \{((a,b),(c,d)) \mid a+b = c+d\}$$

é uma relação de equivalência sobre A^2.

Questão 4.3 Considerando os conjuntos e as relações de equivalência a seguir sobre tais conjuntos, esboce os conjuntos quociente formado por cada relação.

(a). $A = \{a,b,c,d,e\}$ e $R = \{(a,a),(a,e),(b,b),(b,d),(c,c),(d,b),(d,d),(e,a),(e,e)\}$.

(b). $C = \{1,2,3,4\}$ e $S = \{(1,1),(2,2),(3,3),(4,4),(2,4),(4,2)\}$.

(c). $A = \{x \in \mathbb{N} \mid x \leq 20\}$ e $K = \{(x,y) \in A^2 \mid (\exists k \in \mathbb{Z})[\dfrac{(x-y)}{4} = k]\}$.

(d). $D = \{x \in \mathbb{Z} \mid -4 \leq x \leq 5\}$ e $T = \{(x,y) \in D^2 \mid (\exists k \in \mathbb{Z})[\dfrac{(x-y)}{3} = k]\}$.

(e). $E = \{(1,3),(2,4),(0,3),(-4,-8),(3,9),(-1,5),(2,-4),(1,5),(3,6)\}$ e L é a relação definida sobre E da seguinte forma $(x_1,y_1)\ L\ (x_2,y_2)$ se, e somente se, $x_0y_1 = x_1y_0$.

(f). $A = \{-1,0,1\}$ e $M = \{(X,Y) \in \wp(A) \mid num(X) = num(Y)\}$ em que $num(D)$ é o número de elementos em D para qualquer $D \in \wp(A)$.

(g). $N = \{x \in \mathbb{Z} \mid -6 \leq x \leq 6\}$ e $M = \left\{(X,Y) \in \wp(N) \mid \displaystyle\sum_{x \in X} x = \sum_{y \in Y} y\right\}$.

(h). $D = \{x \in \mathbb{Z} \mid -5 \leq x \leq 5\}$ e $T = \{(x,y) \in D^2 \mid (\exists k \in \mathbb{Z})[\dfrac{(x^2-y^2)}{3} = k]\}$.

[8]É esperado que todos os leitores saibam usar as ferramentas de busca da internet para reunir informações necessária sobre os brasileiros ilustres mencionados no Exercício 4.1.

(i). $F = \{x \in \mathbb{Z} \mid -4 \leq x \leq 5\}$ e $T = \{(x, y) \in F^2 \mid (\exists k \in \mathbb{Z})[\dfrac{(x^2 - y^2)}{3} = k]\}$.

(j). $B = \{00, 01, 02, 10, 11, 12, 20, 21, 22\}$ $R = \{(x, y) \in B^2 \mid s(x) = s(y)\}$ onde $s(x)$ denotada a soma dos caracteres para qualquer $x \in B$.

Questão 4.4 Seja A o conjunto de todos os estudantes do seu campus demonstre que a relação T definida sobre A como "$x\ T\ y$ se, e somente se, x é do mesmo curso que y" é uma relação de equivalência.

Questão 4.5 Seja $A = \{a, b, c, d\}$ e $R = \{(a, a), (a, b), (b, a), (b, b), (c, d), (d, c), (d, d), (c, c)\}$. Prove que R é uma relação de equivalência sobre A e esboce também o espaço quociente $A_{/R}$.

Questão 4.6 Sendo R uma relação de equivalência sobre X é correto afirma que $dom(R) = X$?

Questão 4.7 Suponha que R e S são duas relações de equivalência sobre um conjunto A. Prove que $R \cap S$ é também uma relação de equivalência sobre A.

Questão 4.8 Demonstre que a relação $R = \{(x, y) \in \mathbb{Z}^2 \mid x - y \in \mathbb{Z}\}$ é uma relação de equivalência sobre o conjunto $\mathbb{Z}$.

Questão 4.9 Considerando para todo $n \in \mathbb{Z}$ realize o que é solicitado a seguir.

(a). Demonstre que $R_n = \{(x, y) \in \mathbb{Z}^2 \mid \dfrac{x - y}{n} = k\}$ é uma relação de equivalência.

(b). Para o caso particular de $n = 2$ esboce usando notação compacta a classe $[1]$ com respeito a relação R_n.

(c). Para o caso particular de $n = 5$ esboce usando notação compacta a classe $[-4]$ com respeito a relação R_n.

Questão 4.10 Sejam $A = \{1, 2\}$ e $B = \{3, 4\}$ dois elementos de uma partição de $\{1, 2, 3, 4\}$ liste os pares ordenados que compõem a relação de equivalência que definiu a partição que contém A e B.

Questão 4.11 Demonstre que a relação $P = \{(x, y) \in \mathbb{Z}^2 \mid (\exists k \in \mathbb{Z})[x^2 - y^2 = 2k]\}$ é uma relação de equivalência sobre o conjunto $\mathbb{Z}$ e usando notação compacta a classe escreve o espaço quociente gerado por tal relação.

Questão 4.12 Seja $S = \mathbb{N}^2$. Demonstre que a relação $P = \{((x, y), (w, z)) \in S^2 \mid x = z\}$ é uma relação de equivalência sobre o conjunto S e usando notação compacta a classe escreve o espaço quociente gerado por tal relação.

Questão 4.13 Seja $S = \mathbb{Z}^2$. Verifique se a relação $T = \{((x, y), (w, z)) \in S^2 \mid x - y = w - z\}$ é uma relação de equivalência sobre o conjunto S, se for então usando notação compacta a classe escreve o espaço quociente gerado por tal relação.

Questão 4.14 Seja M o conjunto de todas as matrizes simétricas, demonstre que a relação $m_1 K m_2 \iff m_1 = m_2^t$, onde m^t representada a matriz transposta de m com $m \in M$, é uma relação de equivalência.

Questão 4.15 Seja $\sqsubseteq$ uma pré-ordem sobre A:

(a). Demonstre que a relação definida como $\ltimes = \{(x, y) \in A^2 \mid x \sqsubset y \text{ e } y \sqsubset x\}$ é uma relação de equivalência.

(b). Mostre que $\sqsubseteq$ induz (ou gera) uma ordem parcial R sobre $A_{/\ltimes}$ dada por $[x]\ R\ [y]$.

Questão 4.16 Verifique se as seguintes estruturas são *posets*.

(a). $\langle \mathbb{N}, \alpha \rangle$ onde $\alpha = \{(x, y) \in \mathbb{N}^2 \mid$ o resto da divisão de y por x é igual a $1\}$.

(b). $\langle \mathbb{Z}, \alpha \rangle$ onde $\alpha = \{(x, y) \in \mathbb{Z}^2 \mid y = x + 3\}$.

(c). $\langle \mathbb{N}, \alpha \rangle$ onde $\alpha = \{(x, y) \in \mathbb{N}^2 \mid y - x \in \mathbb{N}\}$.

(d). $\langle \mathbb{Z}, \alpha \rangle$ onde $\alpha = \{(x, y) \in \mathbb{Z}^2 \mid 2y - x \in \mathbb{N}\}$.

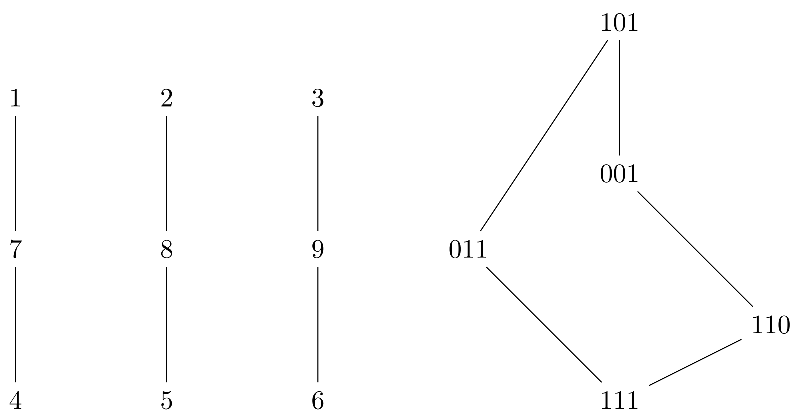
Questão 4.17 Para cada *poset* a seguir desenhe o diagrama um Hasse para o mesmo.

(a). $\langle \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, D \rangle$ onde $x \ D \ y$ se, e somente se, $\dfrac{y}{x} = k$ tal que $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

(b). $\langle \{1, 2, 3\}, \{(1, 1), (1, 2), (2, 2), (3, 3), (1, 3), (2, 3)\} \rangle$.

(c). $\langle \{a, b, c, d\}, \{(d, d), (b, b), (a, a), (c, c), (d, c), (d, a), (a, c)\} \rangle$.

Questão 4.18 Para cada um dos diagrama na Figura 4.13, construa sua estrutura de *poset*.



(a) (b)

Figura 4.13: Diagramas de Hasse para a questão 4.17.

Questão 4.19 Considere o conjunto $X = \{a, b, c, d, e, f, g, h, i\}$ e R a relação de ordem parcial representada pela Figura 4.14, calcule o máximo, mínimo, elementos maximais, elementos minimais, conjuntos dos majorantes, conjuntos dos minorantes, supremo e ínfimo dos seguintes subconjuntos de X:

(a). $A_1 = \{d, e, b\}$.

(b). $A_2 = \{a, c, e, b\}$.

(c). $A_3 = \{g, e, h\}$.

(d). $A_4 = \{d, e, f\}$.

(e). $A_5 = \{a, c, f\}$.

(f). $A_6 = \{a, e\}$.

(g). $A_7 = \{i\}$.

(h). $A_8 = \{d, f, a, i\}$.

(i). $A_9 = \{g, c, b, h\}$.

(j). $A_{10} = \{a, c, f, e\}$.

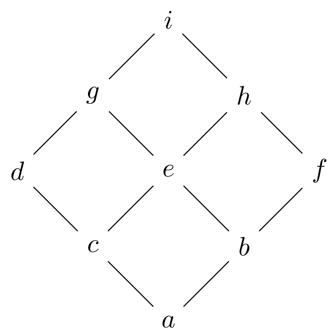


Figura 4.14: Legenda

Questão 4.20 Considere o conjunto $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ e R a relação de ordem parcial representada pela Figura 4.15, calcule o máximo, mínimo, elementos maximais, elementos minimais, conjuntos dos majorantes, conjuntos dos minorantes, supremo e ínfimo dos seguintes subconjuntos de X:

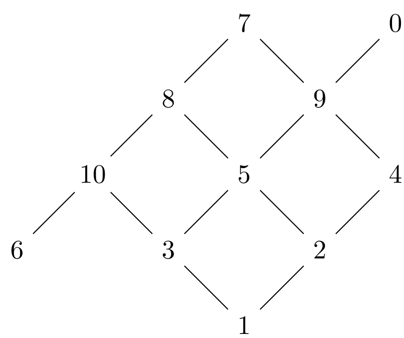


Figura 4.15: Legenda

(a). $A_1 = \{10, 2, 9\}$.

(b). $A_2 = \{0, 6, 4\}$.

(c). $A_3 = \{10, 3, 6, 7\}$.

(d). $A_4 = \{6, 7, 0, 1\}$.

(e). $A_5 = \{9, 8, 3, 2\}$.

(f). $A_6 = \{5, 8, 2\}$.

(g). $A_7 = \{3, 9, 5, 2\}$.

(h). $A_8 = \{10, 1, 4, 7\}$.

(i). $A_9 = \{0, 9, 4, 8\}$.

(j). $A_{10} = \{6, 10, 9, 3, 0, 7\}$.

Questão 4.21 Considere o conjunto $\mathbb{Q}$ ordenado pela ordem usual $\leq$ e seja A um subconjunto de $\mathbb{Q}$ da forma $A = \{x \in \mathbb{Q} \mid x^2 - 2x < 3\}$, o conjunto A é majorado? E ele possui supremo?

Questão 4.22 Considere o conjunto $\mathbb{R}$ ordenado pela ordem usual $\leq$ e seja A um subconjunto de $\mathbb{Q}$ da forma $A = \{x \in \mathbb{Q} \mid x \leq \sqrt{2}\}$, o conjunto A é majorado? E ele possui supremo?

Questão 4.23 Considere um conjunto A qualquer e uma relação binária R sobre A demonstre que R será uma relação de ordem parcial e de equivalência simultaneamente se, e somente se, R for a relação de identidade em A.

Questão 4.24 Dê exemplo de:

(a). Duas relação de ordem parcial sobre um conjunto A, tal que a união das duas não seja uma ordem parcial sobre A.

(b). Duas relação de ordem parcial sobre um conjunto A, tal que a composição das duas não seja uma ordem parcial sobre A.

Questão 4.25 Demostre que se o *poset* $\langle A, \sqsubseteq\rangle$ não tem menor elemento, ou seja, não existe $inf(A)$, então existem no mínimo $x, y \in A$ que são minimais de A.

Questão 4.26 Demostre que se o *poset* $\langle A, \sqsubseteq\rangle$ não tem maior elemento, ou seja, não existe $sup(A)$, então existem no mínimo $x, y \in A$ que são maximais de A.

Questão 4.27 Demostre que se o *poset* $\langle A, \sqsubseteq\rangle$ é tal que $\sqsubseteq$ é uma ordem total, então para todo $x \in A$ existe um único par de elementos $y_1, y_2 \in A$ tal que $y_1 \sqsubseteq x$ e $x \sqsubseteq y_2$.

Questão 4.28 Considerando o conjunto $P = \{t, u, v, w, x, y, z\}$ responda as questões a seguir.

(a). Quantas relações de ordem totais podem ser definida sobre P?

(b). Quantas relações de ordem parcial podem ser definida sobre P de forma que v seja "maior" que w e "menor" que y?

(c). Quantas relações de ordem parcial podem ser definida sobre P de forma que z seja "menor" que y?

Questão 4.29 Para cada conjunto a seguir esboce todas as ordens totais possíveis de serem definidas sobre tais conjuntos.

(a). $\emptyset$

(b). $\{1, -1, a\}$

(c). $\{0, \sqrt{2}, 2\}$

(d). $\{a, b, c, d, e\}$

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

Capítulo 5

Funções

"O ego é o pior inimigo do Eu, mas o Eu é o melhor amigo do ego... O ego é um péssimo senhor, mas é um ótimo servidor".

Bhagavad Gita

5.1 Conceitos, Definições e Nomenclaturas

Após o conceito importantíssimo de conjunto, o componente mais importante na matemática é provavelmente a noção de função. O autor deste documento não hesita em afirmar que você, leitor, com certeza já teve contato com a ideia de função, seja em seus cursos de nível primário, secundário ou mesmo mais recentemente em seus cursos de cálculo diferencial e integral, estatística ou cursos de física.

Dado este encontro anterior do leitor sobre o assunto, o autor fica confortável em pedir que o leitor faça uma pequena pausa e tente lembrar de seus cursos anteriores e responda para si ao questionamento: **o que é uma função**?

Bem, para muitos físicos, estatísticos e alguns matemáticos (não todos[1]), uma função é vista meramente como sendo um mapeamento (ou transformação) entre os elementos de dois conjuntos [1]. Por outro lado, em obras tais como [24, 45, 46, 47, 60] uma função é vista como uma caso particular de relação entre dois conjuntos, ou seja, em última análise para esse grupo de pessoas uma função é exatamente um conjunto[2]. Já em [66, 71] é apresentado uma visão mais mecanicista da ideia de função, essa visão captura a ideia de função enquanto uma máquina[3] (ou caixa

[1]Um visão interessante é aquela apontada em [39], que descreve uma função como sendo um objeto com quatro descrições simultâneas: uma algébrica, uma numérica, uma gráfica e uma descritiva (ou em palavras).

[2]Para melhor entender essa visão talvez o leitor deva revistar os Capítulos 1 e 3 e revisar as definições apresentadas nos mesmo.

[3]Para cientistas da computação os termos máquina e programa são sinônimos.

preta) que transforma as entradas (*inputs*) em saídas (*outputs*), essa visão é ilustrada pela Figura 5.1.

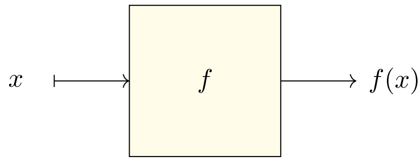


Figura 5.1: Visão de uma função de uma variável enquanto uma máquina (ou caixa preta).

Há também a ideia de função como uma estrutura [28], com componentes bem estabelecidos. Essa visão é capaz (como será mostrado a seguir) de capturar todas as outras ideias de função. Neste documento, a formalização da ideia de função como uma estrutura será apresentada gradualmente, trançando paralelos com as linguagens de programação que possuam um sistema de tipos. Isso será adotado para tornar o texto mais didático e interessante ao leitor de computação, além disso, irá aproximar os tópicos teóricos (as funções) dos tópicos práticos (os programas). Entretanto, essa forma de apresentação não será menos rigorosa que outras fontes bibliográficas. O objetivo deste texto é apresentar da forma mais precisa e detalhada a noção de função, tanto do ponto de vista puramente formal, como do ponto de vista prático (da construção de algoritmos).

Este documento inicia o estudo sobre funções apresentando ao leitor a ideia básica de assinatura de função, isto é, a seguir será apresentado a representação sintática (ou de tipagem) que descreve as funções, ou seja, o componente descritivo como mencionado em [39].

Definição 5.1 — Assinatura de Função. Sejam A e B dois conjuntos a assinatura da função de A em B nomeada como f corresponde a uma palavra da forma $f : A \to B$.

A Definição 5.1 permite facilmente deduzir que em qualquer função existem três elementos básicos, sendo eles: um nome (rótulo ou símbolo funcional), um conjunto de partida e um conjunto de chegada. Por convenção, o nome de uma função deve ser sempre iniciado por caracteres latinos, no caso de usar índices apenas o último caractere do nome deve ser indexado.

Exemplo 5.1 São exemplos de assinaturas de funções:

(a) $g : \mathbb{N} \to \mathbb{Z}$.

(b) $sqrt : \mathbb{R} \to \mathbb{R}$.

(c) $k_1 : A \times B \to \mathbb{C}$.

(d) $loc_2 : D \to \mathbb{R} \times \{0, 1\}$.

(e) $min : \mathbb{R}^n \to \mathbb{R}$.

(f) $BUSCA : \mathbb{Z}^n \times \mathbb{Z} \to \{0, 1\}$.

(g) $BUSCA : \mathbb{R}^n \times \mathbb{R} \to \{0, 1\}$.

(h) $mydouble : \mathbb{Z} \to \mathbb{Z}$.

Observação 5.1 Tenha MUITO cuidado, apesar das assinaturas nos itens (f) e (g) do Exemplo 5.1 terem o mesmo nome, elas não são iguais, pois diferem no conjunto de partida, e assim não são a mesma assinatura. Esse tipo de cenário recebe o nome de sobrecarga[a], isto é, o símbolo funcional $BUSCA$ está sobrecarregado para identificar duas funções distintas.

[a] Na literatura sobre linguagens de programação é usado o termo *override*.

Diversas linguagens de programação tais como C, C++, Haskell e Java (entre outras) apresentam a possibilidade de definir assinaturas de funções. Na linguagem C, por exemplo, as assinaturas de funções que compõem uma biblioteca são geralmente reunidas em um arquivo de *header*, isto é, um arquivo com a extensão ".h", para mais detalhes consulte [26], a seguir é exemplificado um arquivo de *header*.

```c
/* Assinaturas */
int reverse(int x);
int mydouble(int x);
unsigned int strlen (char *x);
int strcmp (char *x, char *y);
char *strcpy (char *y, char *x);
```

Figura 5.2: Exemplo de um arquivo .h contendo assinaturas na linguagem C.

```haskell
-- Assinaturas
mysum :: Int -> Int -> Int
mydouble :: Int -> Int
iseven :: Int -> Bool
factorial :: Int -> Int
```

Figura 5.3: Exemplo de um arquivo com assinaturas na linguagem Haskell.

Um conceito indiretamente esboçado pela ideia de assinatura de função, é o de tipagem da função, sempre que a assinatura é da forma $f : A \to B$ pode-se dizer que f é uma função do tipo "A em B", ou mesmo que "f é um tipo seta de A para B", a noção de "tipo seta" é uma nomenclatura indiretamente ligado a ideia de teoria dos tipos.

Como dito anteriormente uma função pode ser vista como uma máquina que transforma entradas em saídas, mas note que para que isso aconteça a máquina deve de alguma forma realizar ações sobre a entrada, ou seja, a máquina deve "operar" sobre a entrada. Esse conceito de como a máquina deve operar sobre as entradas é descrito por uma propriedade P que define uma relação de mapeamento[4]

Definição 5.2 — Relação de mapeamento. Dado dois conjuntos A e B e seja $x \in A$ e $y \in B$ a relação de mapeamento definida por uma propriedade P corresponde ao seguinte conjunto

$$\varepsilon = \{(x, y) \mid P\}$$

tal que a propriedade P deve satisfazer a seguinte condição: se os pares (x, y_1), (x, y_2) satisfazem P, então obrigatoriamente $y_1 = y_2$.

Note que a Definição 5.2 apenas descreve que para cada entrada (variável) x existirá uma única saída y tal que x e y estão relacionados por uma certa propriedade P.

Exemplo 5.2 São exemplos de relações de mapeamento:

(a) $\{(x, y) \in \mathbb{R}^2 \mid y = \log_2(x + 1)\}\}$

(b) $\{(w_1w_2w_3 \cdots w_m, y) \in E^2 \mid y = w_3 \cdots w_m w_1 w_2\}$ onde E é o conjunto de todas as palavras do português com três letras ou mais e w_i representa o i-ésimo símbolo de uma palavra w.

(c) $\{(x, y) \in \mathbb{N}^2 \mid y = 14\}$.

(d) $\left\{(x_1, x_2, x_3, y) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}_+^* \times \mathbb{R} \mid y = \sqrt[x_3]{\frac{1}{2}x_1 + x_2}\right\}$.

Não são exemplos de relações de mapeamento:

(e) $\{(x, y) \in N_P \times I_P\}$ onde N_P é o conjunto de todos os nomes de pessoas e I_P é o conjunto de naturais que representam idades, note que em tal relação é permitido que $(\text{Fátima}, 10), (\text{Fátima}, 55)$ estejam nesse conjunto, portanto, esse conjunto não satisfaz a Definição 5.2.

(f) $\{(x, y) \in \mathbb{R} \mid x = y^2\}$, note que $(25, 5)$ e $(25, -5)$ pertence a tal conjunto e, portanto, esse conjunto não satisfaz a Definição 5.2.

Tomando Notas 5.1 No item (c) do Exemplo 5.2 descreve que para qualquer x o $y = 14$, ou seja, para todo x tem-se que o par $(x, 14)$ está na relação. Esse tipo de relação de mapeamento será aqui chamada de **relação de mapeamento constante**.

[4]Alguns textos usam a nomenclatura lei de formação, ver por exemplo [14].

Agora que foram apresentados estes conceitos fundamentais pode-se continuar o desenvolvimento deste texto com a formalização da ideia de função.

Definição 5.3 — Função. Dado uma assinatura $f : A \to B$ e seja $\varepsilon \subseteq A \times B$ uma relação de mapeamento, a estrutura $\langle f : A \to B, \varepsilon \rangle$ é uma função.

Exemplo 5.3 São exemplos de funções:

(a) $\langle dob : \mathbb{N} \to \mathbb{N}, \{(x, y) \in \mathbb{N}^2 \mid y = 2x\} \rangle$.

(b) $\langle mul : \mathbb{R} \times \mathbb{R} \to \mathbb{N}, \{((x, y), z) \in \mathbb{R}^2 \times \mathbb{R} \mid z = xy\} \rangle$.

(c) $\langle sqroot : \mathbb{N} \to \mathbb{N}, \{(x, y) \in \mathbb{N}^2 \mid y^2 = x\} \rangle$.

(d) $\langle one : \mathbb{Z}^2 \to \{1\}, \{((x, y), 1) \in \mathbb{Z}^2 \times \{1\} \mid 1 = x + y\} \rangle$.

(e) $\langle sign : \mathbb{R} \to \{0, 1\}, \{(x, y) \in \mathbb{R} \times \{0, 1\} \mid y = 1$ sempre que $x > 0.5$ e $y = 0$ se $x \leq 0.5\} \rangle$.

De forma similar a apresentação feita em [14] aqui será usado a própria relação de mapeamento para definir as noções de domínio e imagem de uma função.

Definição 5.4 — Domínio e Imagem de função. Seja $\langle f : A \to B, \varepsilon \rangle$ uma função o domínio e a imagem de f, denotados respectivamente por $dom(f)$ e $ima(f)$, corresponde exatamente ao domínio e a imagem de ε, ou seja, $dom(f) = Dom(\varepsilon)$ e $ima(f) = Ima(\varepsilon)$.

Exemplo 5.4 Considere a função $\langle k : \mathbb{R} \to \mathbb{R}, \{(x, y) \in \mathbb{R}^2 \mid y = \sqrt{x}\} \rangle$ tem-se que $dom(k) = ima(k) = \mathbb{R}^+$, pois claramente $(x, y) \in \varepsilon$ se, e somente se, $(x, y) = (x, \sqrt{x})$, agora obviamente $\sqrt{x}$ só existe para $x \geq 0$, logo $Dom(\varepsilon) = \mathbb{R}^+$, em contra partida para qualquer seja $\sqrt{x} \in \mathbb{R}$ tem-se que $\sqrt{x} \geq 0$, consequentemente, $Ima(\varepsilon) = \mathbb{R}^+$.

Exemplo 5.5 Considere a função $\langle prev : \mathbb{N} \to \mathbb{N}, \{(x, y) \in \mathbb{N}^2 \mid y = n - 1\} \rangle$, note que $(x, y) \in \varepsilon$ se, e somente se, $(x, y) = (x, x - 1)$, mas $x - 1 \in \mathbb{N}$ apenas se $x > 0$, portanto, tem-se que $dom(prev) = \mathbb{N}_*$. Por outro lado, para qualquer $x > 0$ tem-se que $x - 1 \in \mathbb{N}$ e, portanto, não é difícil verificar que $Ima(\varepsilon) = \mathbb{N}$, consequentemente, $Ima(prev) = \mathbb{N}$.

Agora é comum ao realizar estudos sobre funções, como destacado em [14], não ficar declarando a estrutura da funcional o tempo inteiro (só quando realmente necessário), em vez disso, em geral é descrita a assinatura da função junto com o açúcar sintático (detalhado a seguir), que busca sintetizar todas as informações a cerca da função.

Tomando Notas 5.2 – Açúcar sintático funcional! ALiCIA gostaria que você entenda que para qualquer função $\langle f : A \to B, \varepsilon\rangle$, a notação $f(x)$ é um açúcar sintático para dizer que f está recebendo como entrada x, se escreve $f(x) = y$ como açúcar sintático da frase: "ao calcular f com entrada x é gerado y como saída", mas para isso é necessário que $(x, y) \in \varepsilon$, ou que x e y sejam símbolos de variáveis. Além disso, ALiCIA também observou que quando a relação ε de uma função descreve y a partir de uma igualdade da forma $y = E$, em que E é uma expressão válida, pode-se em vez de, fazer $f(x) = y$ escreve diretamente $f(x) = E$, e desde que $y = E$ a expressão $f(x) = E$ é um refinamento do açúcar sintático.

Exemplo 5.6 Usando as ideias do açúcar sintático descrito na Nota 5.2 tem-se que:

(a) A função $\langle dob : \mathbb{N} \to \mathbb{N}, \{(x, y) \in \mathbb{N}^2 \mid y = 2x\}\rangle$ pode simplesmente ser escrita usando sua assinatura $dob : \mathbb{N} \to \mathbb{N}$ e dizendo que $dob(x) = 2x$.

(b) A função $\langle pot : \mathbb{R} \times \mathbb{N} \to \mathbb{R}, \{((x, y), z) \in (\mathbb{R} \times \mathbb{N}) \times \mathbb{R} \mid z = x^y\}\rangle$ pode simplesmente ser escrita usando sua assinatura $pot : \mathbb{R} \times \mathbb{N} \to \mathbb{R}$ e dizendo que $pot(x, y) = x^y$.

(c) A função $\langle plus4 : \mathbb{N} \to \mathbb{N}, \{(x, y) \in \mathbb{N}^2 \mid y = x + 4\}\rangle$ pode simplesmente ser escrita usando sua assinatura $plus4 : \mathbb{N} \to \mathbb{N}$ e dizendo que $plus4(x) = x + 4$.

Agora com respeito a implementação prática de funções em linguagens de programação, a expressão E mencionada na Nota 5.2 costuma ser chamada de corpo da função em linguagens imperativas, como dito em [65, 50], já nas linguagens funcionais como Haskell, não é nomeada de forma especial, continua sendo mencionada apenas com expressão [44, 51].

Observação 5.2 Deste ponto em diante, quando se for tratar de função abstratamente, sempre que for possível será usado apenas a assinatura para se referir a uma função.

Note que se f é uma função com assinatura $f : A \to B$, isto é, f é um objeto do tipo seta de A em B, e x um objeto do tipo A[5] pode-se pensar em uma regra capaz

[5] Em teoria dos tipos [58, 70] se A é um tipo e x é um objeto do tipo A pode-se escrever que $x : A$, isto é algo semelhante a teoria dos conjuntos ao dizer que $x \in A$.

de deduzir o tipo da saída de $f(x)$, tal regra poderia ser escrita como:

$$\frac{x : A \quad f : A \to B}{f(x) : B}$$

essa regra não é algo novo criado nesse documento, na verdade a mesma, em um certo ponto de vista, é uma versão da famosa regra de *modus ponens*, a existência de tal regra é uma manifestação da profunda conexão que existe entre lógica e computação. Tal conexão é conhecida como isomorfismo de CurryHoward, e é um aspecto fundamental em áreas como teoria dos tipos [58, 70], teoria da prova [58, 67], λ-cálculo [5, 6, 11] e programação funcional [70, 71], este documento irá se aprofundar no estudo de tal isomorfismo em capítulos futuros, quando se estiver estudando λ-cálculo.

```
int sqroot(int x){
  unsigned y = 0;
  while(y*y != x){
    y = y + 1;
  }
  return y;
}
```

Figura 5.4: Código da implementação da função no item (c) do Exemplo 5.3 escrito na linguagem C.

Agora note que a Definição 5.4 não impõe de forma alguma que todos os elementos do conjunto de partida de uma função estejam no seu domínio, e isso gera situação interessantes tanto do ponto de vista teórico quando do ponto de vista prático, para ilustra essa questão considere o código fonte na linguagem C esboçado na Figura 5.4 que implementa a função (c) do Exemplo 5.3 , o que ocorre se tal código receber como entrada um x com valor 3? Bem para um programador com um pouco de experiência nota facilmente que o algoritmo não retorna nada, ficando em *loop* eterno[6]. Para entender essa resposta deve-se atentar aos seguintes fatos:

1. O fato principal é que $\sqrt{3} \notin \mathbb{N}$, ou seja, não existe um $y \in \mathbb{N}$ tal que $y = \sqrt{3}$.

2. A partir do item anterior é claro que não existe um par (x, y) na relação definida pela propriedade $y = \sqrt{x}$ quando $x = 3$.

Assim a função *sqrt* definida no item (c) do Exemplo 5.3 não pode produzir uma saída para a entrada $x = 3$. Do ponto de vista prático (implementação) o programa esboçado na Figura 5.4 encerra e retorna um y como saída se, e somente se, $y = \sqrt{x} \in \mathbb{N}$, dessa forma pode-se pensar que a noção da divergência (ou *loop* eterno) de programas pode ser usada para modelar a indefinição de funções, isto é, quando um programa *prog* é a implementação de um função f sempre que *prog* receber uma entrada para a qual f não calcula uma saída o programa *prog* fica em divergência.

[6] Um simples teste de mesa pode mostra a verdade dessa afirmação, para saber mais sobre testes de mesa ver [50].

Considerando essa pequena discussão pode-se então pensar em separar (ou classificar) as funções, as funções que estão definidas para todas as entradas e as funções que não estão definidas para todas as entradas, essa classificação é formalizada na definição que se segue, tal definição tem uma íntima e importante ligação com a própria teoria da computação [8, 34].

Definição 5.5 — Funções totais e parciais. Uma função $f : A \to B$ é dita ser total sempre que $dom(f) = A$ e será dita parcial sempre que $dom(f) \subseteq A$.

Exemplo 5.7 Considerando as assinaturas $f : \mathbb{Z} \to \mathbb{Z}$, $g, h : \mathbb{N} \to \mathbb{N}$ e $i : \mathbb{R} \to \mathbb{R}_+$ tem-se que:

(a) $f(x) = x - 1$ é uma função total.

(b) $g(x) = \dfrac{1}{x}$ é uma função parcial, visto que $\dfrac{1}{0} \notin \mathbb{N}$.

(c) $h(x) = x^2 + 3$ é uma função total.

(d) $i(x) = x - 5$ é uma função parcial, pois tem-se que $1 - 5 = -4$ e $-4 \notin \mathbb{R}_+$.

Em algumas obras tais como [14], as funções totais também costumam ser chamadas de aplicações, neste documento isto não será feito, aqui será mantido a nomenclatura **função total**. Em texto de teoria da recursão (ou computação) como [9], é comum adotar para as funções parciais a escrita $f(x) = \uparrow$, para denotar que a função f é divergente para entrada x, ou seja, para tal entrada a função não tem uma saída, sempre que necessário será usado nessa notação neste documento.

Exemplo 5.8 Seja $List_{int}$ o conjunto de todas as lista de int da linguagem C, tem-se que a função $first_{int}$ que recebe uma lista de int e retorna o primeiro elemento da mesma não é uma função total, pois se a mesma receber a lista vazia não há um primeiro elemento a ser retornado e assim a mesma deve entrar em divergência.

Observação 5.3 O leitor deve observar que a assinatura de uma função é determinante para a totalidade da mesma, por exemplo, a função f do Exemplo 5.7 com a assinatura $f : \mathbb{N} \to \mathbb{N}$ passa a ser uma função parcial.

Um ponto interessante que talvez o leitor tenha percebido no Exemplo 5.7 é que, para mostrar a parcialidade de uma função basta apresentar um elemento do conjunto de partida para o qual a função em questão não está definida, dessa forma o conjunto de partida é diferente do domínio da função e, portanto, a função é parcial. A seguir é apresentado a definição do espaço de função, um conceito que será importante no decorrer deste documento.

Definição 5.6 — Conjunto ou Espaço de Funções. Sejam A e B conjuntos, o conjunto ou espaço de todas as funções de A em B é denotado[a] por B^A.

[a] Também é encontrado na literatura o uso de $(f : A \to B)$ para denotar o espaço de função [71].

Tomando Notas 5.3 Deste ponto em diante sempre que possível (e não causar ambiguidade) será escrito $f \in B^A$ em vez de escrever a assinatura $f : A \to B$.

Agora que foram estabelecidas as questões de totalidade, parcialidade e espaço das funções, pode-se generalizar a ideia de aplicação de função, e isto é feito introduzido os conceitos de imagem direta e pré-imagem.

Definição 5.7 — Imagem direta e Pré-imagem. Sejam A e B conjuntos e $f \in B^A$, dado dois conjuntos $S \subseteq dom(f)$ e $T \subseteq ima(f)$, a **imagem direta** de f aplicada a S, denotada por $\overrightarrow{f}[S]$, é o conjunto de todos os elementos de B que são gerados a partir da aplicação de f usando os elementos de S como entrada para f, ou seja,

$$\overrightarrow{f}[S] = \{b \in B \mid (\exists x \in S)[f(x) = b]\}$$

dualmente a **pré-imagem** de f aplicada a T, denotado por $\overleftarrow{f}[T]$, corresponde a um subconjunto do domínio de f necessário para "produzir" T como saída da aplicação de f, ou seja,

$$\overleftarrow{f}[T] = \{a \in A \mid (\exists y \in T)[f(a) = y]\}$$

Exemplo 5.9 Considerando uma função $f \in \mathbb{N}^{\mathbb{N}}$ definida como $f(x) = 2x$, tem-se então que $\overrightarrow{f}[\{2, 4, 7\}] = \{14, 8, 4\}$ e $\overleftarrow{f}[\{22, 6, 124\}] = \{3, 11, 62\}$.

Exemplo 5.10 Seja uma função $g \in \mathbb{R}_+^{\mathbb{R}}$ definida como $g(x) = 2x^2 - 1$, dado os conjuntos $A = \{x \in \mathbb{R} \mid 0 < x \leq 2\}$ e $B = \{y \in \mathbb{R}_+ \mid 2 < x < 13\}$ tem-se então a imagem direta:

$$\overrightarrow{f}[A] = \{y \in \mathbb{R}_+ \mid y \leq 7\}$$

e a pré-imagem:

$$\overleftarrow{f}[B] = \left\{x \in \mathbb{R} \mid \sqrt{\frac{3}{2}} < x < \sqrt{7}\right\}$$

da aplicação de f.

Observação 5.4 Cuidado! ALiCIA está brava com o fato de talvez você tenha chegado até aqui sem perceber que, é possível que para algum $S \subseteq A$, $S' \subseteq B$ e $f \in B^A$, tenha-se que: $\overrightarrow{f}[S] = \nexists$, pois para isso (pela Definição 5.7) basta que $S \nsubseteq dom(f)$. Dualmente, pode ser que $\overleftarrow{f}[S'] = \nexists$, bastando para isso que $S' \nsubseteq ima(f)$[a].

[a]O símbolo $\nexists$ é uma outra forma de escrever $\neg\exists$ (não existe).

Exemplo 5.11 Considerando uma função $h \in \mathbb{N}^{\mathbb{N}}$ definida como $h(x) = 2x+1$, tem-se então que $\overrightarrow{h}[\{1, 7, 17, 19\}] = \{3, 15, 35, 39\}$, porém note que, $\overleftarrow{h}[\{0, 15, 5\}] = \nexists$, pois é claro que $h(2) = 5$ e $h(7) = 15$, entrentato, não existe $n \in \mathbb{N}$ tal que $h(n) = 0$, logo o conjunto $\{0, 15, 5\}$ não possui pré-imagem.

Exemplo 5.12 Considere uma função $g \in \mathbb{Z}^{\mathbb{Z}}$ com

$$g(x) = \begin{cases} 1, & \text{se } x = 5k, k \in \mathbb{Z}_+ \\ 0, & \text{se } x = 5j, j \in \mathbb{Z}_- \end{cases}$$

tem-se para a função g que $\overrightarrow{f}[\{3, 7, 12, 4\}] = \nexists$.

Agora observe que a Definição 5.7 estabelece que a imagem direta e a pré-imagem são ambas conjuntos, entretanto, a mesma definição permitir enxergar tais conceitos como funções de fato, para isso pasta notar a seguinte sutiliza, enquanto $f \in B^A$, a imagem direta $\overrightarrow{f}$ pode ser vista como uma função do tipo seta das parte de A nas partes de B, ou seja, $\overrightarrow{f} \in \wp(B)^{\wp(A)}$. Por outro lado, é claro que a pré-imagem $\overleftarrow{f}$ da função f, será uma nova função cujo tipo será seta das parte de B nas partes de A, ou seja, $\overleftarrow{f} \in \wp(A)^{\wp(B)}$.

Proposição 5.1 Dado conjuntos A e B. Se $f \in B^A$ é uma função total, então $\overrightarrow{f} \in \wp(B)^{\wp(A)}$ é uma função total.

Demonstração. Trivial e ficará como exercício ao leitor. □

Definição 5.8 — Igualdade de funções. Duas funções $f, g \in B^A$ são ditas iguais, denotado por $f = g$, sempre que as seguintes condições são satisfeitas.

(i) $dom(f) = dom(g)$ e

(ii) Para todo $x \in dom(f)$ tem-se que $f(x) = g(x)$.

Teorema 5.1 Se $f, g \in B^A$ e $f = g$, então para todo $S \subseteq dom(f)$ tem-se que $\overrightarrow{f}[E] = \overrightarrow{g}[E]$.

Demonstração. Direto da definição 5.8. $\square$

Outro aspecto interessante entre funções que é muito apreciado no estudo (e uso) de linguagens de programação e a ideia de compatibilidade entre funções, esse aspecto é muito importante para algumas linguagens de programação (veja alguns detalhes em [17]), a seguir será expresso formalmente tal conceito.

Definição 5.9 — Compatibilidade de funções. Sejam A e B dois conjuntos e $h_1, h_2 \in B^A$ duas funções, é dito que h_1 e h_2 são compatíveis, sempre que as seguintes propriedades forem satisfeitas:

(i) $dom(h_1) \cap dom(h_2) \neq \emptyset$.

(ii) Para todo $S \subseteq (dom(h_1) \cap dom(h_2))$ tem-se que $\overrightarrow{h_1}[S] = \overrightarrow{h_2}[S]$.

Note que a Definição 5.9 estabelece que duas funções são compatíveis quando elas possuem uma faixa de entradas em comum (ou compartilhada), além disso, é exigido que elas produzam a mesma saída para todos os dados nessa faixa compartilhada. Vale ressaltar que em uma visão de máquina, as duas funções produzirem a mesma saída para os dados, não implica que o funcionamento das duas funções sejam iguais.

Exemplo 5.13 Sejam $f : [0, 1] \to \mathbb{R}$ e $g : \{0, 1\} \to \mathbb{R}$ com $f(x) = \dfrac{1}{x}$ e $g(x) = x^2$ pode-se verificar facilmente que $dom(f) \cap dom(g) = \{1\}$, além disso, é claro que $\overrightarrow{f}[\{1\}] = \{1\} = \overrightarrow{g}[\{1\}]$, portanto, f e g são compatíveis.

Exemplo 5.14 Não é difícil verificar que as funções de $\mathbb{N}$ em $\mathbb{Q}_+$,

$$g(x) = \begin{cases} 2x, & \text{se } x \text{ é par} \\ \dfrac{1}{x-3}, & \text{senão} \end{cases}$$

e $h(x) = \dfrac{4x}{2}$, são tais que $dom(g) \cap dom(h) = \mathbb{N} - \{1, 3\}$. Agora note que $\{5\} \subseteq (dom(g) \cap dom(h))$, por fim, perceba que $\overrightarrow{g}[\{5\}] = \left\{\dfrac{1}{2}\right\}$ e $\overrightarrow{h}[\{5\}] = \{10\}$ e, obviamente $\left\{\dfrac{1}{2}\right\} \neq \{10\}$, consequentemente g e h não são funções compatíveis.

Um ponto importante sobre compatibilidade de duas funções f e g, é o fato que ela (a compatibilidade) só existe na faixa de domínio compartilhada entre duas funções com expresso pela Definição 5.9, entretanto, caso essa faixa coincida como todo o domínio das funções, ou seja, no caso de $dom(f) = dom(g)$ tem-se então que a compatibilidade torna-se exatamente a relação de igualdade entre funções.

5.2 Propriedades das Funções

Esta seção irá tratar de apresentar algumas propriedades que as funções podem apresentar, a saber, as funções pode ser injetora, sobrejetoras e bijetoras[7]. Além disso, aqui também será apresentados alguns resultados importantes sobre as funções envolvendo estas propriedades.

Definição 5.10 — Função injetora. Seja $f \in B^A$, f é dita ser **injetora** sempre que para todo $x_0, x_1 \in dom(f)$, se $x_0 \neq x_1$, então tem-se que $f(x_0) \neq f(x_1)$.

Note que a Definição 5.10 diz que, em uma função f o número de elementos distintos de qualquer subconjunto de $dom(f)$ é sempre mantido na $ima(f)$, ou seja, a saída da função é sempre determinística[8], a Figura 5.5 a seguir ilustra[9] essa ideia, já a função h esboçada pela Figura 5.7 apresenta a característica de que $g(x_2) = g(x_3)$, mas $x_2 \neq x_3$, portanto, h não é injetora[10].

O leitor atento pode perceber que a propriedade de injeção, isto é, a propriedade da função ser injetora, não está ligado ao tipo da função, note que as funções esboçadas nas Figuras 5.5 e 5.6 são ambas injetoras, porém, a primeira é parcial, enquanto que a segunda é total, o Exemplo 5.15 a seguir apresenta algumas funções injetora.

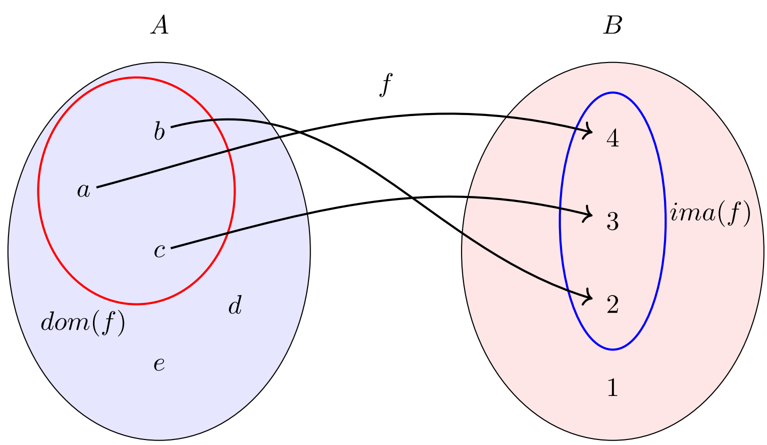


Figura 5.5: Diagrama de uma função f qie é injetora.

[7]Os termos injetora, sobrejetoras e bijetoras foram cunhados e apresentados pela primeiras vez pelo grupo Bourbaki, como explicado em [54].

[8]No sentido de que dois elementos (dados) distintos de entrada sempre irão produz elementos distintos de saída, assim nunca é o caso de não saber que dado geral qual saída.

[9]O Esboço de funções através de diagramas está intimamente ligado ao estudo da teoria dos conjuntos feito pelo matemática inglês John Venn (1834-1923), para detalhes veja [14].

[10]Por não ser injetora a função g esboçada pela Figura 5.7 produz não-determinismo, pois dado apenas a informação de saída y_2 não é possível determinar qual dado de entrada gerou tal saída.

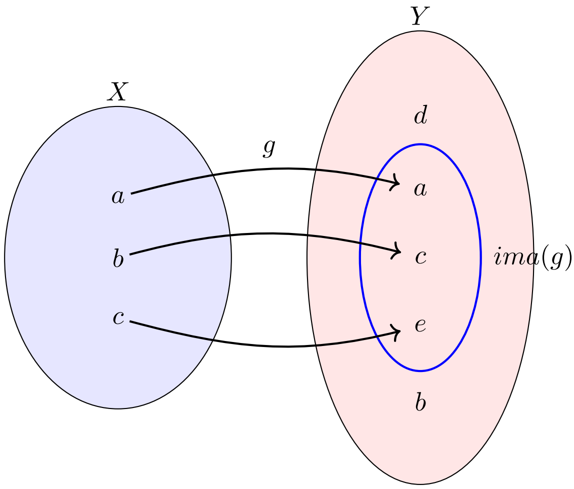


Figura 5.6: Diagrama de uma função injetora g.

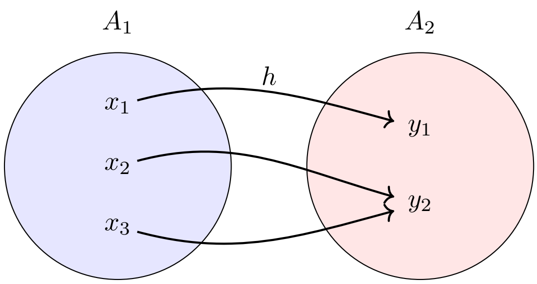


Figura 5.7: Diagrama de uma função h, que não é injetora.

Exemplo 5.15 As funções:

(a) $f(x) = 2x$ com $f \in \mathbb{R}^{\mathbb{Z}}$.

(b) $g(x) = 3x + 1$ com $g \in \mathbb{Z}^{\mathbb{Z}}$.

(c) A função de Cantor $C(x, y) = \dfrac{(x+y)(x+y+1)}{2} + b$ com $C \in \mathbb{N}^{\mathbb{N}\times\mathbb{N}}$.

(d) $Step_k(x) = x + k$ com $k \in \mathbb{Z}_+^*$ e $Step_k \in \mathbb{Z}^{\mathbb{Z}}$.

são todas injetoras. Por outro lado, as funções a seguir não são injetoras.

(e) $T(x, y) = xy$ com $T \in \mathbb{B}^{\mathbb{B}\times\mathbb{B}}$ e $\mathbb{B} = \{0, 1\}$.

(f) $C(x, y) = min(x, y)$ com $C \in L^{L\times L}$ e $L = \{x \in \mathbb{R} \mid 0 \le x \le 1\}$.

(g) $h(x) = x^2$ com $h \in \mathbb{Z}^{\mathbb{Z}}$.

Pela Definição 5.10 pode-se notar que a propriedade de injeção de uma função f é uma propriedade relacionada diretamente com os "dados" de entrada que a função recebe, isto é, a propriedade de injeção está diretamente ligado ao conjunto $dom(f)$. A próxima propriedade que será apresentada, por sua vez, está relacionada ao dados que a função produz após sua aplicação, a mesma relaciona o dados de saída com o conjunto de chega da assinatura da função.

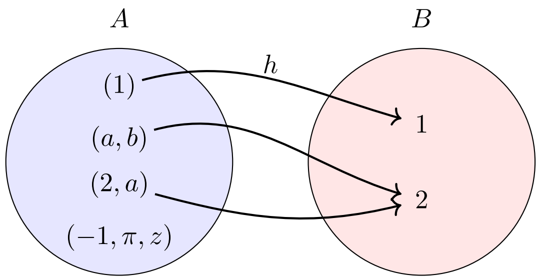


Figura 5.8: Diagrama de uma função h que é sobrejetora.

Definição 5.11 — Função sobrejetora. Seja $f \in B^A$, f é dita ser **sobrejetora** sempre que para todo $y \in B$ existe $x \in A$ tal que $f(x) = y$.

Outra caracterização para funções sobrejetora apresentada em [45] é que, uma função $f \in B^A$ é sobrejetora sempre que $\overrightarrow{f}[dom(f)] = B$, porém, dizer isso é o mesmo que dizer que, uma função $f \in B^A$ é sobrejetora sempre que $ima(f) = B$, que é outra forma de caracterizar funções sobrejetoras como dito em [14]. Claramente a função descrita na Figura 5.7 e 5.8 são ambas sobrejetoras, enquanto as funções esboçadas nas Figuras 5.5 e 5.6 não são sobrejetoras, são também exemplos de funções sobrejetoras os itens $(d), (e)$ e (f) do Exemplo 5.15.

Exemplo 5.16 As funções,

(a) $f(x) = 2x$ com $f \in \mathbb{P}^{\mathbb{N}}$.

(b) $g(x) = \dfrac{1}{x}$ com $g \in L_0^{\mathbb{N}}$ onde $L_0 = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$.

são funções sobrejetoras. Por outro lado, as funções,

(c) $A(x) = 1 - x$ com $A \in \mathbb{N}^{\mathbb{N}}$.

(d) $B(x) = 2x$ com $B \in \mathbb{Z}^{\mathbb{N}}$.

não são funções sobrejetoras.

Definição 5.12 — Função bijetora. Seja $f \in B^A$, f é dita ser **bijetora** sempre que f for total, injetora e sobrejetora.

As funções bijetoras como dito em [45], também costuma ser chamadas de funções biunívocas ou mapeamento um para um (ou *one-to-one* em inglês [14]). Nos casos em que a bijeção $f \in A^A$ para algum conjunto A, a função bijetora f costuma ser chamada de permutação [14] sobre (ou em) A.

Exemplo 5.17 Seja A um conjunto, a função identidade $id_A : A \to A$ construída por $id_A(x) = x$ para todo $x \in A$ é claramente uma bijeção.

Exemplo 5.18 A função descrita pela Figura 5.9 é claramente uma bijeção, uma vez que é visivelmente uma função de um para um.

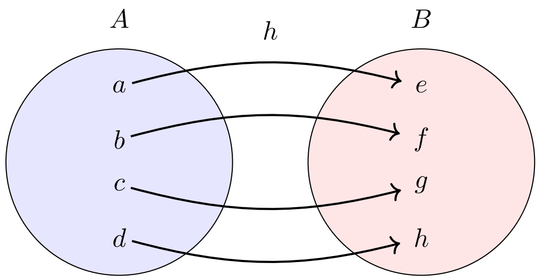


Figura 5.9: Diagrama de uma função h que é bijetora.

Exemplo 5.19 São bijetoras.

(a) A função $f(x) = 2x + 1$ com $f : \mathbb{R} \to \mathbb{R}$.

(b) A função[a] $exp(x)$ com $exp : \mathbb{R} \to \mathbb{R}_+$.

(c) A função C de Cantor, esboçada no item (c) do Exemplo 5.15 é uma bijeção.

(d) A função $r(x) = -x$ com $r \in \mathbb{Z}^{\mathbb{Z}}$ é também uma bijeção[b].

[a] $exp(x)$ é a forma padrão usada principalmente em linguagens de programação e calculadoras científicas para denotar a função exponencial, que na matemática é escrita como e^x sendo e a constante do logaritmo natural.

[b] A função r em algumas obra costuma ser chamada de função de inversão de sinal, pois ela manda todo inteiro positivo x em seu correspondente $-x$, e manda todo $-x$ em sua contraparte positiva.

5.3 Composição e Função Inversa

Como qualquer outro objeto matemático, também existem operações sobre as funções, isto é, mecanismos que atuam sobre funções para criar novas funções. Dessa operações a mais importante é sem dúvidas a composição de funções.

Definição 5.13 — Composição de função. Sejam $f : A \to B$ e $g : B \to C$ duas funções, a função composta de g com f, denotada por $g \circ f$, é uma função com a assinatura $g \circ f : A \to C$ que atende as seguintes restrições:

- $dom(g \circ f) = \{x \mid x \in dom(f) \land f(x) \in dom(g)\}$ e
- $(\forall x \in dom(g \circ f))[(g \circ f)(x) = g(f(x))]$.

Se as funções $f : A \to B$ e $g : B \to C$ forem enxergadas apenas como mapeamentos, a composição das duas funções pode ser vista como sendo uma forma de mapear elementos de A direto em elementos de C, sem há necessidade (explícita) de mapear em B, como ilustrado na Figura 5.10.

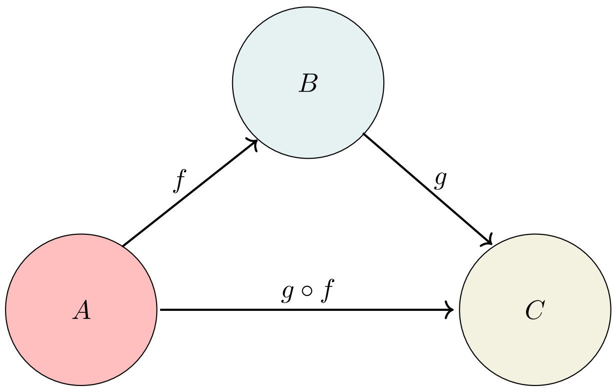


Figura 5.10: Diagrama da composição de uma função g com outra função f.

Por outro lado, a composição vista enquanto máquina (ou caixa preto), e na verdade uma máquina "maior", em que, as funções usadas na composição são apenas partes aninhadas sequencialmente, a Figura 5.11 apresenta essa ideia.

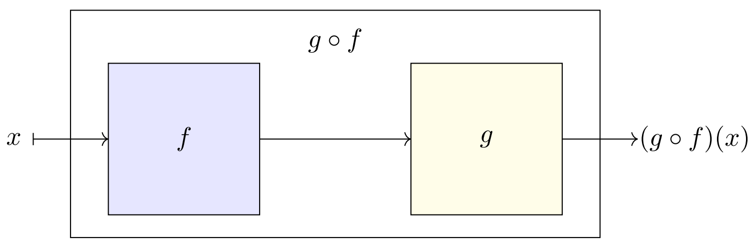


Figura 5.11: Composição $g \circ f$ vista enquanto uma máquina (ou caixa preta).

Agora dado duas funções $f : A \to B$ e $g : B \to C$, com A e B sendo conjuntos numéricos e $f(x) = E$ e $g(x') = E'$ onde E e E' são expressões válidas, e além disso, a expressão E sendo capaz de descrever os elementos em $dom(g)$, tem-se que $(g \circ f)(x) = E'[E/x']$, onde $E'[E/x']$ será uma nova expressão válida obtida a partir da substituição na expressão E' de todas as ocorrências da variável x' pela expressão E.

Exemplo 5.20 Dado a função de naturais em reais $f(x) = \dfrac{1}{x+1}$, e a função de reais em reais $g(x) = (-x+2)^3 + 4$, tem-se que,

$$\begin{array}{rcl} dom(f) & = & \mathbb{N} \\ dom(g) & = & \mathbb{R} \end{array}$$

além disso, tem-se a composição:

$$(g \circ f)(x) = \Big(-\frac{1}{x+1} + 2\Big)^3 + 4$$

note agora que

$$\begin{array}{rcl} dom(g \circ f) & = & \{x \mid x \in dom(f) \wedge f(x) \in dom(g)\} \\ & = & \{x \mid x \in \mathbb{N} \wedge f(x) \in \mathbb{R}\} \\ & = & \mathbb{N} \end{array}$$

e, portanto, a composição $g \circ f$ é uma construção válida.

Exemplo 5.21 Dado duas funções $f_1, f_2 \in \mathbb{Z}^{\mathbb{Z}}$ sendo que $f_1(x) = -x + 3$ e $f_2(x) = 2x + 1$, tem-se que $dom(f_1) = \mathbb{Z}$ e $dom(f_2) = \mathbb{Z}$ assim tem-se que,

(a) $(f_1 \circ f_2)(x) = -2x + 2$ e

(b) $(f_2 \circ f_1)(x) = -2x + 7$.

note agora que,

$$\begin{array}{rcl} dom(f_1 \circ f_2) & = & \{x \mid x \in dom(f_2) \wedge f_2(x) \in dom(f_1)\} \\ & = & \{x \mid x \in \mathbb{Z} \wedge f_1(x) \in \mathbb{Z}\} \\ & = & \mathbb{Z} \end{array}$$

além disso,

$$\begin{array}{rcl} dom(f_2 \circ f_1) & = & \{x \mid x \in dom(f_1) \wedge f_1(x) \in dom(f_2)\} \\ & = & \{x \mid x \in \mathbb{Z} \wedge f_1(x) \in \mathbb{Z}\} \\ & = & \mathbb{Z} \end{array}$$

e, portanto, as composições $f_1 \circ f_2$ e $f_2 \circ f_1$ são ambas construções válidas.

O Exemplo 5.21 é interessante pois ele mostra que a composição de funções não é uma operação comutativa, no sentido de igualdade, ou seja, não é sempre que ocorre que $f_1 \circ f_2 = f_2 \circ f_1$.

Exemplo 5.22 Dado duas funções $i : \mathbb{N} \to \mathbb{Z}$ e $Id_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ tal que $i(x) = -x$ e

$j(x) = \sqrt{x}$, tem-se que a composição $Id_{\mathbb{Z}} \circ i$ não é uma composição válido, pois por definição a aplicação para algum $x \in \mathbb{N}$ seria da forma $(Id_{\mathbb{Z}} \circ i)(x) = Id_{\mathbb{Z}}(i(x)) = \sqrt{-x}$, e obviamente, $\sqrt{-x}$ não é uma expressão válida no contexto dos números inteiros. Note que neste exemplo isso ocorre pelo fato de $-x \notin dom(g)$ com $x \in \mathbb{N}$.

Exemplo 5.23 Dado a função $f(x) = x + 1$ e $g(x) = x - 1$ com $f : \mathbb{N} \to \mathbb{N}$ e $g : \mathbb{Z} \to \mathbb{Z}$, tem-se que $(g \circ f)(x) = g(f(x)) = x$, por outro lado, $f \circ g$ não é um composição válida, pois basta notar que $0 \in dom(g)$, mas $g(0) \notin dom(f)$[a].

[a]Este exemplo considera que $\mathbb{N} \subseteq \mathbb{Z}$ através da ideia de sobrecarga de símbolo, ou seja, todo número natural é sobrecarregado para ser considerado também como número inteiro positivo.

Proposição 5.2 A composição de funções é associativa.

Demonstração. Considere que $f \in B^A, g \in C^B$ e $h \in D^C$, agora pela Definição 5.13 se a composição entre essas funções existe ela irá satisfazer as seguintes pertinência, $g \circ f \in C^A$ e $h \circ (g \circ f) \in D^A$, por outro lado, $h \circ g \in D^B$ e $(h \circ g) \circ f \in D^A$, ou seja, ambas as composições estão no mesmo espaço funcional. Além disso, tem-se que:

$$\begin{aligned}
dom(h \circ (g \circ f)) &\overset{Def. 5.13}{=} \{x \mid x \in dom(g \circ f) \wedge (g \circ f)(x) \in dom(h)\} \\
&\overset{Def. 5.13}{=} \{x \mid x \in \{y \mid y \in dom(f) \wedge f(y) \in dom(g)\} \\
&\qquad \wedge\ (g \circ f)(x) \in dom(h)\} \\
&= \{x \mid x \in dom(f) \wedge f(x) \in dom(g) \wedge g(f(x)) \in dom(h)\}
\end{aligned}$$

Por outro lado, tem-se que:

$$\begin{aligned}
dom((h \circ g) \circ f) &\overset{Def. 5.13}{=} \{x \mid x \in dom(f) \wedge f(x) \in dom(h \circ g)\} \\
&\overset{Def. 5.13}{=} \{x \mid x \in dom(f) \wedge \\
&\qquad f(x) \in \{y \mid y \in dom(g) \wedge g(y) \in dom(h)\}\} \\
&= \{x \mid x \in dom(f) \wedge f(x) \in dom(g) \wedge g(f(x)) \in dom(h)\}
\end{aligned}$$

consequentemente, $dom(h \circ (g \circ f)) = dom((h \circ g) \circ f)$, por fim note que para todo $x \in dom(f)$ segue que,

$$\begin{aligned}
(h \circ (g \circ f))(x) &= h((g \circ f)(x)) \\
&= h(g(f(x))) \\
&= (h \circ g)(f(x)) \\
&= ((h \circ g) \circ f)(x)
\end{aligned}$$

o que conclui a prova. □

A seguir são apresentados mais alguns resultados sobre a composição de funções.

Teorema 5.2 Se $f \in B^A$ é uma função injetora, então existe uma função $g \in A^B$ tal que $(g \circ f)(x) = x$.

Demonstração. Suponha que $f \in B^A$ é uma função injetora, agora deixe $y \in B$. Agora defina uma nova função $g \in B^A$ da seguinte forma:

$$g(y) = \begin{cases} x, & \text{se } f(x) = y \\ a, & \text{senão} \end{cases}$$

para algum $x \in dom(f)$ e $a \in A$. Note que se $y \in ima(f)$, então por f ser injetora irá existir $x \in A$ tal que $f(x) = y$, no caso contrário, é claro que o resultado para $g(y)$ será um $a \in A$ predefinido (ou pré-escolhido), de forma que g é claramente uma função total. Agora note que para todo $x \in dom(f)$ é claro pela contrução de g que $(g \circ f)(x) = g(f(x)) = x$. □

Teorema 5.3 Se $f \in B^A$ é uma função sobrejetora, então existe uma função $g \in A^B$ tal que $(f \circ g)(y) = y$.

Demonstração. A demonstração fica como exercício ao leitor. □

Teorema 5.4 Sejam $f \in B^A$ e $g \in C^B$ duas funções totais, tem-se que:

i. Se f e g são injetoras, então $g \circ f$ também é injetora.

ii. Se f e g são sobrejetoras, então $g \circ f$ também é sobrejetoras.

Demonstração. Dado duas funções totais $f \in B^A$ e $g \in C^B$ tem-se:

i. Suponha que f e g são injetoras, desde que f é total tem-se que para todo $a, a' \in A$ que $f(a)$ e $f(a')$ estão definidos, além disso, como por hipótese f é injetora tem-se para $a \neq a'$ que $f(a) \neq f(a')$, agora por definição de $g \circ f$ todo $f(x) \in ima(f)$ é tal que $f(x) \in dom(g)$, logo $f(a), f(a') \in dom(g)$, como por hipótese g é injetora tem-se que $g(f(a)) \neq g(f(a'))$, ou seja, tem-se que $(g \circ f)(a) \neq (g \circ f)(a')$ e, portanto, $g \circ f$ também é injetora.

ii. A demostração desde item ficará com exercício ao leitor.

□

Corolário 5.1 Se $f \in B^A$ e $g \in C^B$ são bijetoras, então $g \circ f$ também é bijetora.

Demonstração. Direto do Teorema 5.4. □

Teorema 5.5 Dado uma função $f \in B^A$, tem-se que $f \circ id_A = f$ e $id_B \circ f = f$.

Demonstração. Dado uma função qualquer $f \in B^A$ tem-se para todo $x \in dom(f)$ que,

$$(f \circ id_A)(x) = f(id_A(x)) = f(x)$$

ou seja, $f \circ id_A = f$. Por outro lado, considere que para $x \in dom(f)$ tem-se que $f(x) = y$ assim,

$$(id_B \circ f)(x) = id_B(f(x)) = id_B(y) = y = f(x)$$

consequentemente, $id_B \circ f = f$. □

A partir dos conceitos de composição de funções e de funções bijetoras, é possível definir o conceito de inversão para a teoria das funções, ou seja, apresentar o conceito de função inversa. De um ponto de vista operacional, uma função inversa "desfaz" as ações realizadas por uma outra função. A existência da função inversa de funções bijetoras é um corolário direto dos Teoremas 5.2 e 5.3 com dito esboçado em [73].

Definição 5.14 — Função Inversa. Seja $f \in B^A$ uma bijeção, uma função inversa de f é qualquer função $g \in A^B$ tal que $g \circ f = id_{dom(f)}$ e $f \circ g = id_{ima(f)}$, ou seja, para todo $x \in dom(f), y \in ima(f)$ tem-se que $(g \circ f)(x) = x$ e $(f \circ g)(y) = y$.

Agora dado que toda bijeção f é uma função total, as igualdades expressas na Definição 5.14 podem ser reescritas como sendo da forma $g \circ f = id_A$ e $f \circ g = id_B$.

Tomando Notas 5.4 – Apelido da inversa Dado uma função $f \in B^A$, na literatura (ver [46, 47]) é comum usar f^{-1} para se referir a função inversa de f. Além disso, como discutido em [14] se $f \in B^A$ é uma bijeção sua inversa também será uma bijeção.

Exemplo 5.24 Para $f \in \mathbb{R}^{\mathbb{R}}$ com $f(x) = 3x + 4$ tem-se $f^{-1}(x) = \dfrac{(x-4)}{3}$.

Exemplo 5.25 Para $f \in]0,1]^{\mathbb{R}^*_+}$ com $f(x) = \dfrac{1}{x}$ tem-se $f^{-1}(x) = \dfrac{1}{x}$.

Exemplo 5.26 Seja $\mathbb{L}$ o conjunto de todas as listas de números inteiros, a função *doubleend* $\in \mathbb{L}^{\mathbb{L}}$ que dubplica o último elemento na lista l, tem como inversa a função *delatend* $\in \mathbb{L}$ que apaga o último elemento de uma lista.

Exemplo 5.27 Para $f \in \mathbb{N}^{\mathbb{Z}}$ com,

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

tem-se então que $f^{-1} \in \mathbb{Z}^{\mathbb{N}}$ sendo da forma,

$$f^{-1}(x) = \begin{cases} \dfrac{x}{2}, & \text{se } x \in \mathbb{P} \\ -\dfrac{(x+1)}{2}, & \text{senão} \end{cases}$$

Teorema 5.6 Se $f \in B^A$ e $g \in C^B$ são bijetoras, então $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstração. Suponha que $f \in B^A$ e $g \in C^B$ são bijetoras, logo pelo Corolário 5.1 tem-se que $g \circ f$ também é uma bijeção e dado que $g \circ f \in C^A$ tem-se que $(g \circ f)^{-1} \in A^C$, assim,

$$\begin{aligned}
(g \circ f)^{-1} &\overset{Teo.5.5}{=} (g \circ f)^{-1} \circ id_C \\
&\overset{Def.5.14}{=} (g \circ f)^{-1} \circ (g \circ g^{-1}) \\
&\overset{Prop.5.2}{=} ((g \circ f)^{-1} \circ g) \circ g^{-1} \\
&\overset{Teo.5.5}{=} ((g \circ f)^{-1} \circ (g \circ id_B)) \circ g^{-1} \\
&\overset{Def.5.14}{=} ((g \circ f)^{-1} \circ (g \circ (f \circ f^{-1}))) \circ g^{-1} \\
&\overset{Prop.5.2}{=} ((g \circ f)^{-1} \circ ((g \circ f) \circ f^{-1})) \circ g^{-1} \\
&\overset{Prop.5.2}{=} (((g \circ f)^{-1} \circ (g \circ f)) \circ f^{-1}) \circ g^{-1} \\
&\overset{Def.5.14}{=} (id_A \circ f^{-1}) \circ g^{-1} \\
&\overset{Prop.5.2}{=} id_A \circ (f^{-1} \circ g^{-1})
\end{aligned}$$

agora desde que $f^{-1} \in A^B$ e $g^{-1} \in B^C$, tem-se que $f^{-1} \circ g^{-1} \in A^C$ e assim pelo Teorema 5.5 tem-se que $id_A \circ (f^{-1} \circ g^{-1}) = f^{-1} \circ g^{-1}$, o que completa a prova. □

5.4 Famílias

Halmos em [30] menciona que, "... existem diversas ocasiões em que a imagem de uma função é tida como mais importante do que a própria função". Quando este é o caso, a terminologia e a notação, ambas, passam por radicais alterações, que serão introduzidas a seguir.

Definição 5.15 — Família Indexada. Sejam I e D dois conjuntos não vazios, uma família indexada (ou simplesmente família) por I de elementos de D, é uma função injetora e total $u : I \to D$.

A Definição 5.15 estabelece o conceito de família[11], a ideia aqui decorre da seguinte forma, existe um conjunto de índices (ou endereços) I e um conjunto de dados D, a família u é então uma forma de organizar via uso de índices[12] $i \in I$ os elementos armazendos $d \in D$. Aqui cada $u(i)$ é escrito na verdade como u_i, e é chamado de i-ésimo elemento da família. Além disso, a família é representado como $(u_i)_{i\in I}$, em vez de simplesmente usar o símbolo u.

Uma classe de famílias bastante importante na matemática, e por extensão na ciência da computação, são as família ditas como sendo **sequenciais**, esta famílias apresentam a característica de que seu conjunto de índices I é obrigatóriamente uma estrutura de conjunto totalmente ordenado, ou seja, um *poset* onde a ordem é total[13].

Exemplo 5.28 A família sequencial $(f_i)_{i\in\{1,2,3,4,5\}}$ de elementos de $\mathbb{R}$, onde para cada $1 \leq i \leq 5$ o i-ésimo elemento da família é da forma $\dfrac{5+7i}{2i}$, ou seja, $f_i = \dfrac{5+7i}{2i}$.

Exemplo 5.29 A família sequencial $(g_i)_{i\in\mathbb{N}}$ de elementos reais em $[-1,1]$, onde para cada $1 \in \mathbb{N}$ o i-ésimo elemento da família é da forma $f_i = (-1)^i$.

Exemplo 5.30 A família sequencial $(h_i)_{i\in\mathbb{N}}$ de palavras sobre o alfabeto $\{a,b,c\}$, onde para cada $1 \in \mathbb{N}$ o i-ésimo elemento da família será da forma $a^i b^{2i} c^i$, ou seja, $h_i = a^i b^{2i} c^i$. Ressaltando que aqui, para todo $x \in \{a,b,c\}$ a notação x^i diz respeito a uma palavra formada por i-repetições de x, ou seja, $x^i = \underbrace{x \cdots x}_{i-\text{vezes}}$.

Tomando Notas 5.5 – Família Sequenciais na Programação Um conceito importante presente na maioria das linguagens de programação é a estrutura de dados chamada *array* (vetor em português) [26, 50, 65, 69], na verdade tais estruturas são uma implementação computacional da noção de família. Por exemplo, na linguagem C um *array* chamando *values* de 5 números do tipo *int*, na verdade é uma implementação de uma família da forma $(values)_{i\in\{0,1,2,3,4\}}$, em que a imagem de *values* é um conjunto de valores do tipo *int*. É interessante notar que $values_i$ é representado na linguagem C por $values[i]$.

Outra classe de famílias que é bastante importante, são as família ditas como

[11] Obras como [30] e [14] também mencionam a nomeclatura indexação.
[12] Ou seja, uma família estabelece o conceito de chave-valor, tão importante dentro das linguagens de programação.
[13] Se necessário releia a Seção 4.4 do Capítulo 4 para relembrar deste conceito

sendo **não sequenciais**, esta famílias apresentam a característica de que seu conjunto de índices I não é visto como sendo uma estrutura de conjunto parcialmente (ou totalmente) ordenado, ou seja, o importa no conjunto de índices são os elementos em si, e não a relação existente entre eles.

Exemplo 5.31 A família $(e_i)_{i\in\{r,1,c,-1\}}$ de elementos de $\mathbb{R}\cup T$ onde T é o conjunto de nomes de rua e cidades do Brasil, onde a família é da forma:

- $e_r =$ Rua Prefeito José Pereira da Silva.
- $e_1 = 79$.
- $e_c =$ Jaçanã-RN.
- $e_{-1} = 0$.

Exemplo 5.32 A família $(b_i)_{i\in\{id,v,d\}}$ de elementos de $\mathbb{N}\cup N$ onde N é o conjunto de nomes de clubes da primeira divisão do campeonato espanhou, onde a família é então da forma:

- $b_{id} =$ Barcelona.
- $b_v = 74$.
- $b_d = 78$.

As famílias não sequenciais são particularmente importante para as linguagens de programação, pois são essas famílias que descrevem matematicamente o conceito de **registros** (ou **estruturas**) presentes nas linguagens de programação, o exemplo a seguir ilustra o uso deste tipo de família na linguagem de programação C.

```
#ifndef USER_H
#define USER_H

typedef struct {
  char* nome;
  char tipousuario;
  unsigned matricula;
  unsigned idade;
} user;

#endif
```

Figura 5.12: Exemplo de um arquivo .h que especifica um novo tipo user.

Exemplo 5.33 Considere a tarefa de modelar um usuário em um sistema de gerenciamento escolar, o usuário ao se cadastrar no sistema deve informa: nome, e-mail, id do tipo de usuário, número de matricula e idade. Na linguagem C o usuário pode ser modelado pelo novo tipo de dados chamado *user* que é definido no trecho de código na Figura 5.12. Assim um usário novo criado no sistema será uma nova variável P do tipo *user*, ou seja, um usuário chamado P é na verdade uma implementação de uma família $(P_{i \in \{nome, tipousuario, matricula, idade\}})$. Note que uma instrução da forma $P.nome =$ "João″ é a implementação em C de $P_{nome} =$ João da família.

Tomando Notas 5.6 Uma coisa interessante a se destacar no Exemplo 5.33 é que a imagem de qualquer família[a] é sempre um subconjunto finito do universo discurso char* $\cup$ char $\cup$ unsigned. Obviamente, com essa visão, é necessário extrapolar nos tipos da linguagem C para serem visto como conjunto.

[a]Variaveis instanciadas do tipo pessoa.

A ideia de família possibilita também apresentar uma forma generalizada de algumas operações entre conjuntos como, por exemplo, a união e intersecção. Essas operações recebem apenas dois conjuntos como argumentos, entretanto é possível generalizá-las para uma quantidade qualquer de argumentos fazendo o uso de famílias de conjuntos.

Definição 5.16 Seja U um universo do discurso e seja $\{A_i\}_{i \in I}$ uma família tal que para todo i tem-se que $A_i \subseteq U$. A união da família de conjuntos $\{A_i\}_{i \in I}$, denotada por $\bigcup\limits_{i \in I} A_i$, corresponde ao conjunto de todos os $x \in U$ tal que existe $i \in I$ de forma que $x \in A_i$, matematicamente tem-se que:

$$\bigcup_{i \in I} A_i = \{x \in U \mid (\exists i \in I)[x \in A_i]\}$$

Exemplo 5.34 Seja $A_1 = \{a, b, c\}$, $A_2 = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$ e $A_3 = \{1, a, 2\}$ os elementos da família $\{A_i\}_{i \in \{1,2,3\}}$ tem-se que:

$$\begin{aligned} \bigcup_{i \in \{1,2,3\}} A_i &= A_1 \cup A_2 \cup A_3 \\ &= \{a, b, c\} \cup \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\} \cup \{1, a, 2\} \\ &= \{a, b, c, \spadesuit, \clubsuit, \heartsuit, \diamondsuit, 1, 2\} \end{aligned}$$

Apesar da Definição 5.16 não apresentar de forma explícita, a união generalizada em uma família só é possível quando o conjunto dos índices é um conjunto recursivamente enumerável, com discutido em [14]. De forma dual é possível definir a ideia de intersecção generalizada, sobre uma família de conjuntos.

Definição 5.17 Seja U um universo do discurso e seja $\{A_i\}_{i\in I}$ uma família tal que para todo i tem-se que $A_i \subseteq U$. A intersecção da família de conjuntos $\{A_i\}_{i\in I}$, denotada por $\bigcap_{i\in I} A_i$, corresponde ao conjunto de todos os $x \in U$ tal que existe $i \in I$ de forma que $x \in A_i$, matematicamente tem-se que:

$$\bigcap_{i\in I} A_i = \{x \in U \mid (\forall i \in I)[x \in A_i]\}$$

Exemplo 5.35 Seja C_1 um elemento de uma família $\{C_i\}_{i\in\{1,2\}}$, onde C_1 que representa o código das disciplinas do primeiro semestre de um curso de ciência da computação da forma,

$$C_1 = \{cc0133, cc0131, cc0134, cc0132, cc0135, cc0136\}$$

e seja C_2 o elemento da família que representa o código das disciplinas do primeiro semestre de um curso de engenharia computação com a forma,

$$C_2 = \{ec1011, ec1012, cc0131, cc0134, ec1013, ec1015\}$$

tem-se então que:

$$\begin{aligned}
\bigcap_{i\in\{1,2\}} C_i &= C_1 \cap C_2 \\
&= \{cc0133, cc0131, cc0134, cc0132, cc0135, cc0136\} \cap \\
&\quad \{ec1011, ec1012, cc0131, cc0134, ec1013, ec1015\} \\
&= \{cc0131, cc0134\}
\end{aligned}$$

5.5 Questionário

Questão 5.1 Construa uma assinatura de função, para cada enunciado a seguir.

(a). f é uma função que mapeia um par de pessoa e uma pessoa.

(b). g é uma função que transforma um número natural em outro número natural.

(c). h é uma função que pega quatro números reais e devolve um par de números racionais onde o segundo número do par não pode ser zero.

(d). i é a função que dado uma figura bidimensional devolve o número de lados da figura.

(e). j é a função que mapeia os números reais no intervalo $[0, 1]$ para os números inteiros positivos.

(f). k é uma função que mapeia uma matriz quadrada de tamanho $n \times n$ para um vetor de tamanho n.

```c
#ifndef ASSINATURAS_H
#define ASSINATURAS_H

int somar(int a, int b);
float calcularMedia(float* valores, int tamanho);
int checarMensagem(char* mensagem);
int maximo(int a, int b, int c);
double calcularAreaCirculo(double raio);
int contarCaracteres(char* string);
int arrayOrdenado(int* array, int tamanho);
float converterParaCelsius(float temperaturaFahrenheit);
int fatorial(int numero);
int matrizNaNula(int** matriz, int linhas, int colunas);
char* concatenarStrings(char* str1, char* str2);
void abrirArquivo(char* nomeArquivo, char* modo);
int verificarPrimo(int numero);
int copiarVetor(int* origem, int* destino, int tamanho);
double calcularPotencia(double base, int expoente);
int dadosValidos(char* nome, int* idade, float* altura);
int encontrarIndiceValor(int* array, int tamanho, int valor);
int aprovado(float a, float b, float c);
char* gerarSenhaAleatoria(int comprimento);

#endif
```

Figura 5.13: Um arquivo .h contendo assinaturas na linguagem C.

(g). l é a função que associa uma lista de palavras sobre um determinado alfabeto, a uma lista de seus respectivos comprimentos.

(h). m é a função que recebe como entrada um conjunto de pontos no plano cartesiano e retorna o ponto médio desses pontos.

(i). n é a função que recebe um gráfico de uma função matemática e retorna o valor máximo local dessa função.

Questão 5.2 Para cada assinatura de função da linguagem C apresenta na Figura 5.13 implemente dois corpos de função de forma que em um a função seja total e em outro a função seja parcial.

Questão 5.3 Determine o domínio e a imagem de cada função a seguir.

(a). $f(x) = 2x$, com assinatura $f : \mathbb{R} \to \mathbb{R}$.

(b). $g(x) = \dfrac{1}{x}$, com assinatura $g : \mathbb{R} \to \mathbb{R}$.

(c). $h(x) = \sqrt{x}$, com assinatura $h : \mathbb{R} \to \mathbb{R}$.

(d). $f(n) = \dfrac{1}{n}$, com assinatura $f : \mathbb{Z} \to \mathbb{Z}$.

(e). $g(n) = n^2$, com assinatura $g : \mathbb{Z} \to \mathbb{Z}$.

(f). $h(n) = n!$, com assinatura $g : \mathbb{Z} \to \mathbb{Z}$.

(g). $f(x) = \sin(x)$, com assinatura $f : \mathbb{R} \to \mathbb{R}$.

(h). $g_2(x) = \dfrac{1}{x^2}$, com assinatura $g_2 : \mathbb{R} \to \mathbb{N}$.

(i). $h_2(x) = \log(x)$, com assinatura $h_2 : \mathbb{R} \to \mathbb{R}$.

(j). $s(x, y) = x + y$, com assinatura $s : \mathbb{Z}^2 \to \mathbb{R}$.

(k). $p(x, y) = \dfrac{x}{y}$, com assinatura $s : \mathbb{N}^2 \to \mathbb{R}$.

(l). $m(x, y) = x^y$, com assinatura $m : \mathbb{R}_+ \times \mathbb{Z} \to \mathbb{R}$.

(m). $n(x, y) = \dfrac{1}{x}$, com assinatura $n : (\mathbb{Z} - \{0, 1\}) \times \mathbb{Z} \to \mathbb{Q}$.

(n). $k(x) = \sqrt{x - 1}$, com assinatura $k : \mathbb{Z} \to \mathbb{Z}$.

(o). $l(x) = \log(x - 2)$, com assinatura $l : \mathbb{Q} \to \mathbb{R}$.

(p). $v(n) = (-1)^n$, com assinatura $v : \mathbb{Z} \to \mathbb{Z}$.

(q). $t(x) = \dfrac{1}{x - 1}$, com assinatura $t : \mathbb{N} \to \mathbb{Q}$.

(r). $w(x, y) = \dfrac{x}{y}$, com assinatura $w : \mathbb{R}^2 \to \mathbb{R}$.

(s). $h(x, y) = \log(x - y)$, com assinatura $h : \mathbb{R}^2 \to \mathbb{R}$.

Questão 5.4 Verifique (Demonstre) se as funções a seguir são totais ou parciais.

(a). $f(x, y, z) = x^2 + y^2 + z^2$, com assinatura $f : \mathbb{R}^3 \to \mathbb{R}$.

(b). $g(x, y, z) = \dfrac{x}{yz}$, com assinatura $g : \mathbb{Z}^3 \to \mathbb{Q}$.

(c). $h(x, y) = \sqrt{2 - xy}$, com assinatura $f : \mathbb{N}^2 \to \mathbb{N}$.

(d). $i(x, y, z) = x + y - z$, com assinatura $i : \mathbb{R}^3 \to \mathbb{R}$.

(e). $j(x, y, z) = \dfrac{x}{y + z}$, com assinatura $j : \mathbb{Z}^3 \to \mathbb{Q}$.

(f). $k(x, y, z) = \sqrt[3]{x^2 + y^2 + z^2}$, com assinatura $k : \mathbb{R}^3 \to \mathbb{R}$.

(g). $l(x, y, z) = \dfrac{x}{y + z} - \dfrac{z}{x - y}$, com a assinatura $k : \mathbb{Z}^3 \to \mathbb{Q}$.

(h). $m(x) = \sqrt{x}$, com assinatura $m : \mathbb{N} \to \mathbb{N}$.

(i). $n(x, y) = 2x - \sqrt{x}$, com assinatura $n : \mathbb{R} \times \mathbb{N} \to \mathbb{N}$.

Questão 5.5 Determine (caso existam) as imagens diretas e pré-imagens de cada conjunto com respeitos as funções nos cenários descritos nas questões a seguir.

(a). Dado os conjuntos $\{1, 23, 13\}, \{41, 3\}$ e $\{0, 25, 5, 125, 115\}$ e seja $f : \mathbb{N} \to \mathbb{N}$ a função $f(x) = 2x + 3$.

(b). Dado os conjuntos $\{p \mid 11 < p \leq 117\}, \{3, 5, 7, 9, 11, 13, 17\}$ e $\{2^p + 1 \in \mathbb{N} \mid p \in \mathbb{N}\}$ e seja $g : \mathbb{N} \to \mathbb{N}$ uma função da forma $g(n) = n^2$.

(c). Dado os conjuntos $\{25, 19, 0, 12\}$ e $\{k \in \mathbb{N} \mid 5 \leq k < 99\}$ e sendo $f, g : \mathbb{N} \to \mathbb{N}$ duas funções definidas como $f(x) = x + 3$ e $g(x) = x + 2 \cdot f(x + 1)$.

(d). Dado os conjuntos $\{-1, 23, -13, 7, 5, -7, -11, -9, 0, 41, 3\}$ e $\{z \in \mathbb{Z} \mid z = 5d, d \in \mathbb{Z}\}$ e seja $f : \mathbb{Z} \to \mathbb{N}$ a função $f(x) = x^2 + 1$.

(e). Dado $\{x \in \mathbb{Z} \mid -122 < x \leq 122\}$ e $\{x \in \mathbb{Z} \mid -12 < x \leq 12\} - \{2, 3, 4, 5, 7\}$ e sendo $g : \mathbb{Z} \to \mathbb{N}$ uma função da forma $g(t) = t^2 - 4$.

(f). Dado $\{5, 7, 19\}, \{2y \in \mathbb{N} \mid y \in \mathbb{N}\}$ e $\{y^2 - 1 \in \mathbb{N} \mid y \in \mathbb{N}\}$ e seja a $h : \mathbb{N} \to \mathbb{N}$ a função $f(x) = 3x - 1$.

(g). Dado os conjuntos $\{125, -19, 0, -122, 3\}$, $\{k \in \mathbb{Z} \mid k = 2i + 1, -17 < i < 17\}$ e $\mathbb{N}$ e sejam $h_1 : \mathbb{Z} \to \mathbb{R}$ e $h_2 : \mathbb{R} \to \mathbb{R}$ duas funções definidas como $h_1(x) = \dfrac{x}{2}$ e $h_2(x) = h_1(x) + 1$.

(h). Dado o conjunto $\{x \in \mathbb{R} \mid -99 < x < 100\}$ e $f : \mathbb{R} \to \mathbb{R}$ a função $f(x) = \dfrac{1}{x}$.

Questão 5.6 Dado os conjuntos $A = \{x \in \mathbb{R} \mid -4 < x < 4\}$ $B = \{p \in \mathbb{R} \mid 0 \leq p \leq 12\}$ e $C = \{i \in \mathbb{R} \mid -25 \leq i < 0\}$, e sejam $f, g : \mathbb{R} \to \mathbb{R}$ duas funções tais que $f(x) = \sqrt{x}$ e $g(x) = x^2$. Calcule e esboce (caso existam) $\overleftarrow{k_i}[X]$, $\overrightarrow{k_i}[X]$, com $i \in \{1, 2\}$ e $X \in \{A, B, C\}$, ressaltando que, $k_1, k_2 : \mathbb{R} \to \mathbb{R}$ definidas respectivamente como sendo $k_1(x) = 1 + f(x) - 2g(x)$ e $k_2(x) = \dfrac{g(x)}{f(x)}$.

Questão 5.7 Construa 4 exemplos de funções de naturais em naturais, de naturais em reais e de reais em reais que sejam compatíveis entre si.

Questão 5.8 Diga se as funções a seguir são (apenas) injetoras, (apenas) sobrejetoras, bijetoras ou se não são nem injetoras e nem sobrejetoras, justifique suas respostas.

(a). $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ tal que $f(x) = 3$ para todo $x \in \{1, 2, 3, 4, 5\}$.

(b). $g, h : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ tal que a aplicação de g e h são descritas pela Tabela 5.1.

x	1	2	3	4	5
$g(x)$	2	3	1	5	4
$h(x)$	1	4	1	1	3

Tabela 5.1: Aplicação da função g do item (b) da questão 5.8

(c). $h : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ com $h(x) = 6 - x$.

(d). $i : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ com

$$i(x) = \begin{cases} \dfrac{x}{2}, & \text{se } x \text{ é par} \\ \dfrac{x+1}{2}, & \text{senão} \end{cases}$$

Questão 5.9 Usando a representação de tabela (veja o item (b) da Questão 5.8) exiba todas as funções totais distintas[14] possíveis do $\{1,2,3,4,\}$ para o conjunto $\{a,b,c\}$, depois diga quais são injetoras, sobrejetoras e bijetoras.

Questão 5.10 De três exemplo de funções pertencentes a $\mathbb{N}^{\mathbb{N}}$ que:

(a). São bijetoras.

(b). São injetoras, mas não sobrejetoras.

(c). São sobrejetoras, mas não injetoras.

(d). Não são injetoras e nem sobrejetoras.

Questão 5.11 De três exemplo de funções pertencentes a $\mathbb{R}^{\mathbb{R}}$ que:

(a). São bijetoras.

(b). São injetoras, mas não sobrejetoras.

(c). São sobrejetoras, mas não injetoras.

(d). Não são injetoras e nem sobrejetoras.

Questão 5.12 Dado a função $f(x) = x^2 + 2$ com $f \in \mathbb{R}^{\mathbb{R}}$

(a). A função é injetora? Justifique sua resposta.

(b). A função é sobrejetora? Justifique sua resposta.

(c). Calcule (se existir) $\overrightarrow{f}[A]$ com $A = [4,6]$ e $\overrightarrow{f^{-1}}[\{1\}]$.

(d). Calcule (se existir) $\overleftarrow{f}[\{6,28,12\}]$ e $\overrightarrow{f^{-1}}[\{0,28,12\}]$.

Questão 5.13 Seja A e B dois conjuntos não vazios e seja $f : A \to B$ uma função total, demonstre que:

(a). Se $A \subseteq B$, então $\overrightarrow{f}[A] \subseteq \overrightarrow{f}[B]$.

(b). Se $A \subseteq B$, então $\overrightarrow{f^{-1}}[A] \subseteq \overrightarrow{f^{-1}}[B]$.

Questão 5.14 Sobre composição de funções responda o que é solicitado a seguir.

(a). Dado $f, g \in \mathbb{R}^{\mathbb{R}}$ com $f(x) = \dfrac{1}{\sqrt{x+1}}$ e $g(x) = x^2$, determine $f \circ g$ e $g \circ f$.

[14] Distintas aqui é sinônimo de diferentes, veja a noção de igualdade de função (Definição 5.8) caso necessite.

(b). Dado $f, g, h \in \mathbb{R}^{\mathbb{R}}$ com $f(x) = |x|, g(x) = \dfrac{x+1}{x-1}$ e $h(x) = 3^x - 1$, esboce as funções $f \circ g, g \circ f, h \circ g, g \circ h, g \circ g$ e $(g \circ f) \circ h$.

Questão 5.15 Dado $f : A \to B$ demonstre que $f \circ Id_A = Id_B \circ f$.

Questão 5.16 Apresente a inversa de cada função a seguir.

(a). $f(x) = 7x + 3$ com $f : \mathbb{Q} \to \mathbb{Q}$.

(b). $g(x) = 4 - 3x$ com $g : \mathbb{Z} \to \mathbb{Z}$.

(c). $h(x) = \dfrac{3x+2}{2x-5}$ com $h : \mathbb{R} - \{\dfrac{5}{2}\} \to \mathbb{R}$.

(d). $i(x) = x^3 - \dfrac{1}{3^x}$ com $i : \mathbb{R} \to \mathbb{R}$.

(e). $j(x) = \dfrac{2x+6}{x-4}$ com $j : \mathbb{Q} - \{4\} \to \mathbb{Q}$.

Questão 5.17 Dado um conjunto A e uma família $\{G_i\}_{i\in I}$ demonstre que:

(a). Se $A \in \{G_i\}_{i\in I}$, então $A \subseteq \bigcup\limits_{i\in I} G_i$.

(b). Se $A \in \{G_i\}_{i\in I}$, então $\bigcap\limits_{i\in I} G_i \subseteq A$.

Questão 5.18 Demonstre que: se B é um conjunto e $\{G_i\}_{i\in I}$ uma família para todo $i \in I$ tem-se que se $B \subseteq A_i$, então $B \subseteq \bigcap\limits_{i\in I} G_i$.

Questão 5.19 Demonstre que: se $\{G_i\}_{i\in I}$ é uma família e $\emptyset = G_i$ para algum $i \in I$, então $\bigcap\limits_{i\in I} G_i = \emptyset$.

Capítulo 6

Cardinalidade

"Que ninguém seja capaz de nos tirar do paraíso que Cantor criou para nós"

David Hilbert

Capítulo 7

Indução

> *"Indução Matemática é a técnica de prova padrão na Ciência da Computação."*
>
> *Anthony Ralston*

7.1 Introdução

No Capítulo 2 foram apresentados diversos métodos para a demonstração de asserções, além disso, foram apresentadas técnicas para refutar enunciados falaciosos. Neste capítulo será apresentado um outro método de demonstração chamando **indução matemática**, ou simplesmente indução.

A indução apresenta uma característica extremamente interessante que não é encontrada em outros métodos de demonstração, sendo esta característica a capacidade de fornecer uma estratégia de construção extremamente forte para estruturas abstratas da Ciência da Computação (e matemática), de tal forma que as propriedades dessas estruturas geradas são relativamente fáceis de serem demonstradas ou verificadas.

No que tange a historia o primeiro ao utilizar da indução para realizar uma demonstração foi o matemático italiano Francesco Maurolico (1494–1575), depois nos séculos seguintes nomes como Pierre de Fermat[1] (1607–1665) e Blaise Pascal[2] (1623–1662) usaram tal método de demonstração em seus trabalhos, como dito em [24] nas próximas seções serão apresentados os conceitos ligados a demonstrações por indução e ao processo de construção indutiva.

[1] Famoso por suas contribuições em geometria e teoria dos números.
[2] Entre outras contribuições criou a máquina analítica.

7.2 Indução como Método de Demonstração

Para demonstrar que uma determinada propriedade **P** acontece para qualquer que seja o número natural n, denotado por $\mathbf{P}(n)$, usando indução é necessário aplicar o conceito chamado de "**princípio da indução finita**", este conceito é em geral apresentado de duas forma: **fraca**[3] e **forte**. A seguir é formalmente definido a versão fraca de tal princípio.

Definição 7.1 — Princípio da Indução Fraca. Dado $\mathbf{P}(n)$ uma condição (ou propriedade) definida sobre os números naturais. Se

(i) $\mathbf{P}(0)$ é verdadeira e

(ii) qualquer que seja k tem-se que, se $\mathbf{P}(k)$ é verdadeira, então $\mathbf{P}(k+1)$ também é verdadeira.

Então, para todo $n \in \mathbb{N}$ tem-se que $\mathbf{P}(n)$ é verdadeiro.

Em termos da escrita usada na lógica de primeira ordem (ver **??**) o princípio da indução fraca é da forma $(\mathbf{P}(0) \wedge (\forall k \in \mathbb{N})[\mathbf{P}(k) \Rightarrow \mathbf{P}(k+1)]) \Rightarrow (\forall n \in \mathbb{N})[\mathbf{P}(n)]$. O procedimento (ou método) de se demonstrar alguma propriedade por indução consiste em, informar que a prova será feita usado indução, depois deve-ser usar os três passos descritos na definição, sendo tais passos:

(B)ase: Neste passo é provado que a proposição vale para 0, ou seja, deve-se provar que $\mathbf{P}(0)$ realmente é verdadeira.

(H)ipótese indutiva: Supor que $\mathbf{P}(k)$ é verdadeira para um valor k genérico.

(P)asso indutivo: Demonstrar que $\mathbf{P}(k+1)$ também é verdadeira.

Após isso pode-se concluir que a propriedades que se está verificado é verdadeira para todos os naturais [14]. A razão pela qual o princípio da indução pode ser usado para demonstrar propriedades dos números naturais decorre do fato de como os naturais são construídos, na Seção 7.4 será apresentada uma forma axiomática desta construção, vale entretanto ressaltar que a indução pode ser empregado em qualquer conjunto que seja recursivamente enumerável.

Tomando Notas 7.1 A partir deste ponto será denotado por $P(n) := \varepsilon$, a noção que a propriedade $P(n)$ corresponde a expressão ε aplicando a variável n.

No que se segue serão apresentados alguns exemplos sobre a aplicação do método de demonstração por indução (versão fraca).

[3]Também é possível encontrar na literatura a nomenclatura "forma simples".

Exemplo 7.1 Seja $r \in \mathbb{N} - \{0, 1\}$ e $a \in \mathbb{R}$, considere que $P(n) := ar^0 + ar + \cdots + ar^n = \dfrac{a(r^{n+1} - 1)}{r - 1}$ e demonstre que $(\forall n \in \mathbb{N})[P(n)]$.

Demonstração. A prova será feita por indução sobre os naturais, assim note que:

(B)ase: Por um lado é claro que $ar^0 = a \cdot 1 = a$, por outro lado tem-se que, $\dfrac{a(r^{0+1} - 1)}{r - 1} = \dfrac{a(r^1 - 1)}{r - 1} = a$, assim pela transitividade de $=$ segue que $ar^0 = \dfrac{a(r^{0+1} - 1)}{r - 1}$ e, portanto, $\mathbf{P}(0)$ é verdadeiro.

(H)ipótese indutiva: Suponha que $P(k)$ seja verdadeira para qualquer $k \in \mathbb{N}$, logo tem-se que $ar^0 + ar + \cdots + ar^k = \dfrac{a(r^{k+1} - 1)}{r - 1}$.

(P)asso indutivo: Agora note que:

$$\begin{array}{rcl} ar^0 + ar + \cdots + ar^k + ar^{k+1} & = & (ar^0 + ar + \cdots + ar^k) + ar^{k+1} \\ & \overset{(\mathbf{H})}{=} & \dfrac{a(r^{k+1} - 1)}{r - 1} + ar^{k+1} \\ & = & \dfrac{a(r^{k+1} - 1)}{r - 1} + \dfrac{ar^{k+1}(r - 1)}{r - 1} \\ & = & \dfrac{a(r^{k+1} - 1)}{r - 1} + \dfrac{ar^{k+2} - ar^{k+1}}{r - 1} \\ & = & \dfrac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r - 1} \\ & = & \dfrac{a(r^{k+2} - 1)}{r - 1} \end{array}$$

consequentemente $P(k + 1)$ é verdadeira. Agora desde que k em **(H)** e **(P)** é um elemento genérico qualquer de $\mathbb{N}$ e também pelo resultado particular em **(B)** pode-se dizer para todo $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira. □

Exemplo 7.2 Demonstre para todo $n \in \mathbb{N}$ que $P(n)$ é verdadeira, considerando que $P(n) := 2^{n-1} \leq n!$.

Demonstração. A prova será feita por indução sobre o conjunto dos naturais. Assim observe que:

(B)ase: Inicialmente é claro que $2^{0-1} = 2^{-1} = \dfrac{1}{2}$, além disso, por definição tem-se que $0! = 1$, e é sabido que $\dfrac{1}{2} \leq 1$, consequentemente $2^{0-1} \leq 0!$ e, portanto, $P(0)$ é verdadeira.

(H)ipótese indutiva: Suponha que $P(k)$ seja verdadeira para qualquer

$k \in \mathbb{N}$, ou seja, tem-se que $2^{k-1} \leq k!$.

(P)asso indutivo: Primeiro considerando também a hipótese adicional H_0 de que $k \geq 1$ tem-se que:

$$\begin{array}{rcl} (k+1)! & = & (k+1) \cdot k! \\ & \overset{\textbf{(H)}}{\geq} & (k+1) \cdot 2^{k-1} \\ & \overset{H_0}{\geq} & 2 \cdot 2^{k-1} \\ & = & 2^k \end{array}$$

ou seja, tem-se que $2^k \leq (k+1)!$. Por outro lado, o caso em que é considerada a hipótese adicional H_1 de que k seja exatamente igual a 0 é trivial (fica como exercício), assim a conclui-se a argumentação mostrando que para qualquer que seja k tem-se que $P(k+1)$ será verdadeira. Agora por **(B)**, **(H)** e **(P)** pode-se efetivamente enunciar que para todo $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira. $\square$

Exemplo 7.3 Considerando que $P(n) := \displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, demonstre para todo $n \in \mathbb{N}$ que $P(n)$ é verdadeira.

Demonstração. A prova será feita por indução sobre o conjunto dos naturais. Assim observe que:

(B)ase: Inicialmente é claro que $\dfrac{0(0+1)}{2} = 0$, além disso, por definição tem-se que $\displaystyle\sum_{i=0}^{0} i = 0$, consequentemente, pela transitividade da igualdade tem-se que $\displaystyle\sum_{i=0}^{0} i = \frac{0(0+1)}{2}$ e, portanto, $P(0)$ é verdadeira.

(H)ipótese indutiva: Suponha que $P(k)$ seja verdadeira para qualquer $k \in \mathbb{N}$, ou seja, tem-se que $\displaystyle\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$.

(P)asso indutivo: Agora note que:

$$\begin{aligned}\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^{k} i\right) + (k+1)\\ &\overset{(\mathbf{H})}{=} \frac{k(k+1)}{2} + (k+1)\\ &= \frac{(k+1)(k+2)}{2}\\ &= \frac{(k+1)((k+1)+1)}{2}\end{aligned}$$

consequentemente $P(k+1)$ é verdadeira. Agora desde que k em **(H)** e **(P)** é um elemento genérico qualquer de $\mathbb{N}$ e também pelo resultado particular em **(B)** pode-se dizer para todo $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira. □

Exemplo 7.4 Considerando que $P(n) := \sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ onde $r \in \mathbb{R}$ tal que $r \neq 1$, demonstre para todo $n \in \mathbb{N}$ que $P(n)$ é verdadeira.

Demonstração. A prova será feita por indução sobre o conjunto dos naturais. Assim observe que:

(B)ase: Inicialmente é claro que para qualquer $r \in \mathbb{R}$ com $r \neq 1$ tem-se que $\frac{r^{0+1}-1}{r-1} = 1$, além disso, por definição tem-se que $\sum_{i=0}^{0} r^0 = 1$, consequentemente, pela transitividade da igualdade tem-se que $\sum_{i=0}^{0} r^i = \frac{r^{0+1}-1}{r-1}$ e, portanto, $P(0)$ é verdadeira.

(H)ipótese indutiva: Suponha que $P(k)$ seja verdadeira para qualquer $k \in \mathbb{N}$, ou seja, tem-se que $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$.

(P)asso indutivo: Agora note que:

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \left(\sum_{i=0}^{k} r^i\right) + r^{k+1} \\
&\overset{(\mathbf{H})}{=} \frac{r^{k+1}-1}{r-1} + r^{k+1} \\
&= \frac{r^{k+1}-1+r^{k+2}-r^{k+1}}{r-1} \\
&= \frac{r^{k+2}-1}{r-1}
\end{aligned}$$

o que mostra que $P(k+1)$ é verdadeira. Agora desde que k em **(H)** e **(P)** é um elemento genérico qualquer de $\mathbb{N}$ e também pelo resultado particular em **(B)** pode-se dizer para todo $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira. □

Agora como dito em [14], em algumas situações para se provar por indução é necessário supor uma hipótese indutiva mais forte. Nesses casos é interessante (e até necessário) supor que $P(0), \cdots, P(k)$ são todas verdadeiras, em vez de, supor apenas que $P(K)$ seja verdadeira. Quando tal suposição é feito, é dito que se está demonstrado usando o princípio forte da indução.

Definição 7.2 — Princípio da Indução Forte. Dado $\mathbf{P}(n)$ uma condição (ou propriedade) definida sobre os números naturais. Se

(i) $\mathbf{P}(0)$ é verdadeira e

(ii) qualquer que seja k tem-se que, se $\mathbf{P}(0), \cdots, \mathbf{P}(k)$ são verdadeiras, então $\mathbf{P}(k+1)$ também é verdadeira.

Então, para todo $n \in \mathbb{N}$ tem-se que $\mathbf{P}(n)$ é verdadeiro.

Usando a escrita da lógica de primeira ordem, o princípio da indução forte pode ser especificado da seguinte forma, $(\mathbf{P}(0) \wedge (\forall k \in \mathbb{N})[(\forall i \leq k)[\mathbf{P}(k)] \Rightarrow \mathbf{P}(k+1)]) \Rightarrow (\forall n \in \mathbb{N})[\mathbf{P}(n)]$. Utilizando o conceito de sequência apresentado no Capítulo **??**, pode-se dizer que na indução forte assume-se que uma sequência de hipótese é totalmente verdadeira, ou seja, que todas as hipóteses na sequência $(\mathbf{P}(i))_{i \leq k}$ são verdadeiras.

A seguir serão apresentados alguns exemplos sobre o uso da estratégia de indução forte como um método de demonstração, depois nas próximas seções serão apresentados respectivamente a equivalência entre a indução fraca e forte, e alguns cuidados que devem ser tomados ao se usar indução.

Exemplo 7.5 Considerando que $P(n)$:= "Seja $a = (a_n)_{n \in \mathbb{N}}$ satisfazendo as conduções:

- $a_0 = 1$

- $a_1 = 3$
- $a_{n+1} = 2a_n - a_{n-1}$ para todo $n \geq 1$.

tem-se que $a_n = 2n + 1$ para qualquer que seja $n \in \mathbb{N}$". Demonstre que $(\forall n \in \mathbb{N})[P(n)]$ é verdadeira.

Demonstração. Utilizando o princípio da indução forte sobre os naturais tem-se que:

(B)ase: Pela definição da sequência tem-se que $a_0 = 1$, mas desde que $2 \cdot 0 + 1 = 1$, tem-se pela transitividade da igualdade que $a_0 = 2 \cdot 0 + 1$.

(H)ipótese indutiva: Suponha para $k \in \mathbb{N}$ que $P(0), \cdots, P(k)$ são todas verdadeiras, ou seja, $a_i = 2i + 1$ para todo $0 \leq i \leq k$.

(P)asso indutivo: Agora note que:

$$\begin{aligned} a_{k+1} &\overset{Def.}{=} 2a_k - a_{k-1} \\ &\overset{\textbf{(H)}}{=} 2(2k+1) - (2(k-1)+1) \\ &= 4k + 2 - 2k + 2 - 1 \\ &= 4k - 2k + 3 \\ &= 2k + 3 \\ &= 2(k+1) + 1 \end{aligned}$$

Consequentemente $P(k+1)$ é verdadeiro. Agora desde que k em **(H)** e **(P)** é um elemento genérico qualquer de $\mathbb{N}$ e também pelo resultado particular em **(B)** pode-se concluir que para qualquer que seja $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira, concluindo assim a prova. □

Exemplo 7.6 Considerando que $P(n) :=$ "Seja $a = (a_n)_{n \in \mathbb{N}}$ satisfazendo as conduções:

- $a_0 = 7$
- $a_1 = 16$
- $a_{n+1} = 5a_{n-1} - 6a_{n-2}$ para todo $n \geq 1$.

assim $a_n = 5 \cdot 2^n + 2 \cdot 3^n$ para qualquer que seja $n \in \mathbb{N}$". Demonstre que $(\forall n \in \mathbb{N})[P(n)]$ é verdadeira.

Demonstração. Utilizando o princípio da indução forte sobre os naturais tem-se que:

(B)ase: Note que por definição da sequência tem-se que $a_0 = 7$, mas desde que $7 = 5 \cdot 2^0 + 2 \cdot 3^0$, tem-se pela transitividade da igualdade que $a_0 = 5 \cdot 2^0 + 2 \cdot 3^0$ e, portanto, $P(0)$ é verdadeira.

(H)ipótese indutiva: Suponha para $k \in \mathbb{N}$ que $P(0), \cdots, P(k)$ são todas verdadeiras, ou seja, $a_i = 5 \cdot 2^i + 2 \cdot 3^i$ para todo $0 \leq i \leq k$.

(P)asso indutivo: Agora note que:

$$\begin{aligned}
a_{k+1} &\overset{Def.}{=} 5a_{(k+1)-1} - 6a_{(k+1)-2} \\
&= 5a_k - 6a_{k-1} \\
&\overset{\textbf{(H)}}{=} 5(5 \cdot 2^k + 2 \cdot 3^k) - 6(5 \cdot 2^{k-1} + 2 \cdot 3^{k-1}) \\
&= 25 \cdot 2^k + 10 \cdot 3^k - 30 \cdot 2^{k-1} - 12 \cdot 3^{k-1} \\
&= 25 \cdot 2^k + 10 \cdot 3^k - 30 \cdot 2^k \cdot 2^{-1} - 12 \cdot 3^k \cdot 3^{-1} \\
&= 25 \cdot 2^k - 15 \cdot 2^k + 10 \cdot 3^k - 4 \cdot 3^k \\
&= 10 \cdot 2^k + 6 \cdot 3^k \\
&= 5 \cdot 2^{k+1} + 2 \cdot 3^{k+1}
\end{aligned}$$

Consequentemente $P(k+1)$ é verdadeiro. Agora desde que k em **(H)** e **(P)** é um elemento genérico qualquer de $\mathbb{N}$ e também pelo resultado particular em **(B)** pode-se concluir que para qualquer que seja $n \in \mathbb{N}$ tem-se que $P(n)$ é verdadeira, o que terminar a prova. □

Agora é claro, como discutido em [14], que é praticamente natural considerar o princípio da indução fraca como sendo um caso particular do princípio da indução forte, entretanto, essa consideração não deve "cegar" a mente do leitor, ao induzir-lo a acreditar que a versão forte seja mais poderosa que a versão fraca, no que tange a isto, os seguintes resultados bem conhecidos a seguir mostram que na verdade ambos os princípios tem um mesmo poder de demonstração.

Teorema 7.1 [14] Dado A é um conjunto de naturais. Se é verificável pelo princípio da indução fraca uma propriedade P dos elementos de A, então a propriedade P dos elementos de A é verificável pelo princípio da indução forte.

Teorema 7.2 [14] Dado A é um conjunto de naturais. Se é verificável pelo princípio da indução forte uma propriedade P dos elementos de A, então a propriedade P dos elementos de A é verificável pelo princípio da indução fraca.

Corolário 7.1 O princípio da indução fraca é equivalente ao princípio da indução forte.

Demonstração. Direto dos Teoremas 7.1 e 7.2. □

Agora esta seção irá se dedicar a tarefa de apresentar ao leitor a relação existente entre o conceito de indução finita e a noção de conjunto bem ordenado, isto é, aqui será tratado da relação íntima que existe entre o princípio de indução e os conjuntos sobre os quais pode-se definir uma relação de boa ordem.

Teorema 7.3 Todo subconjunto não vazio de $\mathbb{N}$ tem mínimo.

Demonstração. Suponha por absurdo que existe um $B \subseteq \mathbb{N}$ não vazio tal que B não tem mínimo. Agora seja $A = \{i \in \mathbb{N} \mid (\forall x \in B)[i \leq x]\}$, ou seja, $A \subseteq B$. Agora por indução tem-se que:

> **(B)**ase: $0 \in A$, pois é claro que $0 \leq x$ tal que $x \in B$.
>
> **(H)**ipótese indutiva: Suponha para todo $k \in \mathbb{N}$ que $k \in A$.
>
> **(P)**asso indutivo: Pelo fato em **(H)** sabe-se que $k \notin B$ uma vez que por hipótese B não tem mínimo, assim é claro que $k < x$ para todo $x \in B$, mas de $k < x$ pode-se concluir que $k+1 \leq x$ e, portanto, $k+1 \in A$

Agora é claro por **(B)**, **(H)** e **(P)** que $A = \mathbb{N}$, e assim desde que $B \subseteq \mathbb{N}$ existe um $k \in A \cap B$ e, portanto, $A \cap B \neq \emptyset$, logo existe um k que é um mínimo de B uma vez que $k \leq x$ para todo $x \in B$, o que é um absurdo uma vez que por hipótese B não tem mínimo, consequentemente, a asserção: todo subconjunto não vazio de $\mathbb{N}$ tem mínimo, é verdadeira. □

Teorema 7.4 Se $\mathbb{N}$ é bem ordenado, então para qualquer $A \subseteq \mathbb{N}$ tem-se que se

(i) $0 \in A$.

(ii) qualquer que seja $n \in \mathbb{N}^*$, se $\{k \in \mathbb{N} \mid k < n\} \subseteq A$, então $n \in A$.

Então $A = \mathbb{N}$.

Demonstração. Suponha por absurdo que $\mathbb{N}$ é bem ordenado e para qualquer $A \subseteq \mathbb{N}$ tem-se que (i) e (ii) são satisfeitas e $A \neq \mathbb{N}$. Agora por $A \subseteq \mathbb{N}$ e $A \neq \mathbb{N}$ tem-se claramente que $\mathbb{N} - A \neq \emptyset$, e por $\mathbb{N}$ ser bem ordenado, existe um $i = min(\mathbb{N} - A)$, agora por (i) é claro que $0 \in A$, e assim como $i \in \mathbb{N} - A$ tem-se que obrigatoriamente que $i \neq 0$, mas $0 = min(\mathbb{N})$, consequentemente tem-se que $0 \leq i$ e, portanto, $0 < i$. Agora uma vez que $i = min(\mathbb{N} - A)$ tem-se que não existe nenhum $j \in \mathbb{N} - A$ tal que $j < i$. Logo é claro que $\{j \in \mathbb{N} \mid j < i\} \subseteq A$, mas como $i > 0$, por (ii), fica evidente que $i \in A$, o que é um absurdo uma vez que $i = min(\mathbb{N} - A)$, assim pode-se concluir que o enunciado do Teorema 7.4 é verdadeiro. □

7.3 Indução Bem fundada

Escrever depois . . .

7.4 Estruturas Indutivamente Geradas

Escrever depois . . .

Referências Bibliográficas

[1] J. M. Abe and N. Papavero. *Teoria Intuitiva dos Conjuntos.* MAKRON *Books*, 1991.

[2] U. R. Acharya, P. S. Bhat, S. S. Iyengar, A. Rao, and S. Dua. Classification of heart rate data using artificial neural network and fuzzy equivalence relation. *Pattern recognition*, 36(1):61–68, 2003.

[3] A. V. AHO, M. S. LAM, R. SETHI, and J. D. ULLMAN. *Compiladores: Princípios, Técnicas e ferramentas.* Editora Pearson, 2 edition, 2007.

[4] A. Bar-Hillel, T. Hertz, N. Shental, and D. Weinshall. Learning distance functions using equivalence relations. In *Proceedings of the 20th international conference on machine learning (ICML-03)*, pages 11–18, 2003.

[5] H. P. Barendregt. *The Lambda Calculus Its Syntax and Semantics.* Elsevier, 1984.

[6] H. P. Barendregt. *Lambda Calculi with Types.* Oxford: Clarendon Press, 1992.

[7] J. M. Barreto, M. Roiseberg, M. A. F. Almeida, and K. Callozos. *Fundamentos de Matemática Aplicada à Informática.* `http://www.inf.ufsc.br/~mauro.roisenberg/ine5381/leituras/apostila.pdf`, Universidade Federal de Santa Catarina, ????–2021. Work in progress.

[8] B. Bedregal, B. M. Acióly, and A. Lyra. *Introdução à Teoria da Computação: Linguagens Formais, Autômatos e Computabilidade.* Editora UnP, Natal, 2010.

[9] B. R. C. Bedregal and S. Figueira. Classical computability and fuzzy turing machines. In *Latin American Symposium on Theoretical Informatics*, pages 154–165. Springer, 2006.

[10] Y. Bertot and P. Castéran. *Interactive Theorem Proving and Program Development: CoqArt: The Calculus of Inductive Constructions.* Springer Science & Business Media, 2013.

[11] K. Bimbó. *Combinatory Logic: Pure, Applied and Typed,.* Chapman and Hall/CRC, 2019.

[12] K. Broda, J. Ma, G. Sinnadurai, and A. Summers. Pandora: A reasoning toolbox using natural deduction style. *Logic Journal of the IGPL*, 15(4):293–304, 2007.

[13] G. Cantor. Beiträge zur Begründung der Transfiniten Mengenlehre. *Mathematische Annalen*, 46(4):481–512, 1895.

[14] J. Carmo, P. Gouveia, and F. M. Dionísio. *Elementos de Matemática Discreta*. College Publications, 2013.

[15] M. E. Celebi. *Partitional clustering algorithms*. Springer, 2014.

[16] K. Cooper and L. Torczon. *Construindo Compiladores*, volume 1. Elsevier Brasil, 2017.

[17] C. I. Corporation. Compatible functions (C only). Acessado em 17 de Julho de 2023 na página https://www.ibm.com/docs/en/zos/2.4.0?topic=definitions-compatible-functions-c-only, 2021.

[18] V. S. Costa. Linguagens Lineares Fuzzy. Master's thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2016.

[19] V. S. Costa. *Autômatos Fuzzy Hesitantes Típicos: Teoria e Aplicações*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2020.

[20] N. Cressie and J. L. Davidson. Image analysis with partially ordered markov models. *Computational statistics & data analysis*, 29(1):1–26, 1998.

[21] E. de Alencar Filho. *Iniciação à Lógica Matemática*. NBL Editora, 2002.

[22] A. A. de Lima. *Conjuntos fuzzy multidimensionais*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.

[23] S. S. Epp. *Discrete mathematics with applications*. Wadsworth Publ. Co., 1990.

[24] S. S. Epp. *Discrete Mathematics With Applications*. Cengage learning, 2010.

[25] A. D. S. Farias, V. S. Costa, R. H. Santiago, and B. Bedregal. The image reduction process based on generalized mixture functions. In *2016 Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS)*, pages 1–6. IEEE, 2016.

[26] P. Feofiloff. *Algoritmos em linguagem C*. Elsevier Brasil, 2009.

[27] X. Z. Fern and C. E. Brodley. Solving cluster ensemble problems by bipartite graph partitioning. In *Proceedings of the twenty-first international conference on Machine learning*, page 36, 2004.

[28] J. L. Gersting. *Fundamentos Matemáticos para Ciência da Computação*. GrupoGen LTC, 2021.

[29] D. Giri and P. Srivastava. A cryptographic key assignment scheme for access control in poset ordered hierarchies with enhanced security. *Int. J. Netw. Secur.*, 7(2):223–234, 2008.

[30] P. R. Halmos. *Teoria ingênua dos conjuntos.* Editora Ciência Moderna, 2001.

[31] R. Hammack. *Elements of Discrete Mathematics.* Virginia Commonwealth University Richmond Virginia, 1.1 edition, 2017.

[32] F. Hausdorff. *Grundzüge der mengenlehre*, volume 7. von Veit, 1914.

[33] L. Hegenberg. *Lógica: Cálculo Sentencial, Cálculo de Predicados, Cálculo com Igualdades.* GEN, 3ł edition, 2012.

[34] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to Automata Theory, Languages and Computation.* Pearson Education India, USA, 3ł edition, 2008.

[35] E. Karaman, M. Soyertem, İ. Atasever Güvenç, D. Tozkan, M. Küçük, and Y. Küçük. Partial order relations on family of sets and scalarizations for set optimization. *Positivity*, 22(3):783–802, 2018.

[36] P. J. Landin. The mechanical evaluation of expressions. *The computer journal*, 6(4):308–320, 1964.

[37] P. J. Landin. Correspondence between algol 60 and church's lambda-notation: part i. *Communications of the ACM*, 8(2):89–101, 1965.

[38] P. J. Landin. A correspondence between algol 60 and church's lambda-notations: Part ii. *Communications of the ACM*, 8(3):158–167, 1965.

[39] O. Levin. *Discrete mathematics: An open introduction.* 2021.

[40] X. Li, X. Huang, Z. Nie, and Y. Zhang. Equivalent relations between inter-channel coupling and antenna polarization coupling in polarization diversity systems. *IEEE transactions on antennas and propagation*, 55(6):1709–1715, 2007.

[41] T. Y. Lin. Data mining: Granular computing approach. In *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, pages 24–33. Springer, 1999.

[42] P. Lingras and Y. Yao. Data mining using extensions of the rough set model. *Journal of the American society for information science*, 49(5):415–422, 1998.

[43] P. Linz. *An Introduction to Formal Languages and Automata.* Jones & Bartlett Learning, USA, 2006.

[44] M. Lipovaca. *Learn you a haskell for great good!: a beginner's guide.* no starch press, 2011.

[45] S. Lipschutz. *Topologia Geral.* McGRAW-HILL Do Brasil, LTDA/MEC, 1971. Coleção Schaum.

[46] S. Lipschutz. *Teoria dos Conjuntos*. McGraw-Hill do Brasil - LTDA/MEC, 1978.

[47] S. Lipschutz and M. Lipson. *Matemática Discreta*. Bookman Editora, 2013. Coleção Schaum.

[48] J. P. Martins. *Lógica e Raciocínio*. College Publications, 2014.

[49] Y. V. Matiyasevich, J. V. Matijasevič, Û. V. Matiâsevič, Y. V. Matiyasevich, Y. V. Matiyasevich, M. R. Garey, and A. Meyer. *Hilbert's tenth problem*. MIT press, 1993.

[50] M. Medina and C. Ferting. *Algoritmos e Programação: Teoria e Prática*. Novatec Editora, 2006.

[51] A. S. Mena. *Beginning Haskell: A Project-Based Approach*. Apress, 2014.

[52] P. B. Menezes. *Matemática Discreta para Computação e Informática*, volume 2. Bookman, 2010.

[53] T. R. B. Milfont. *Grafos fuzzy intervalares n-dimensionais*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2021.

[54] J. Miller. Earliest Known Uses of Some of the Words of Mathematics (I). Acessado em 22 de Agosto de 2023 na página https://jeff560.tripod.com/i.html, 2023.

[55] J. Morgado. *Introdução à Teoria dos Reticulados, Textos de Matemática*. Instituto de Física e Matemática, Recife, 1962.

[56] L. d. Moura, S. Kong, J. Avigad, F. v. Doorn, and J. v. Raumer. The lean theorem prover (system description). In *International Conference on Automated Deduction*, pages 378–388. Springer, 2015.

[57] V. V. Myasnikov. Description of images using a configuration equivalence relation. *Computer Optics*, 42(6):998–1007, 2018.

[58] R. Nederpelt and H. Geuvers. *Type theory and formal proof: an introduction*. Cambridge University Press, 2014.

[59] J. Neggers and H. S. Kim. *Basic posets*. World Scientific, 1998.

[60] G. O'Regan. *Guide to discrete mathematics*. Springer, 2021.

[61] R. E. B. Paiva. *Uma extensão de overlaps e naBL-Álgebras para reticulados*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.

[62] B. C. Pierce, C. Casinghino, M. Gaboardi, M. Greenberg, C. Hriţcu, V. Sjöberg, and B. Yorgey. *Matemática Fundacional para Computação*. https://softwarefoundations.cis.upenn.edu/, University of Pennsylvania, 2007.

[63] A. J. Pinheiro. *On algebras for interval-valued fuzzy logic*. PhD thesis, Programa de Pós-graduação em Sistemas e Computação, Universidade Federal do Rio Grande do Norte, UFRN, Natal, RN, 2019.

[64] R. Pressman and B. Maxim. *Engenharia de Software*. McGraw Hill Brasil, 8ł edição edition, 2016.

[65] Python Software Foundation. Página oficial da linguagem Python. Acessado em 23 de Agosto de 2023 na página https://www.python.org/, 2023.

[66] E. R. Scheinerman. *Matemática Discreta - Uma Introdução*. Cengage Learning Editores, terceira edição edition, 2019.

[67] I. Sergey. Programs and proofs: Mechanizing mathematics with dependent types. *Lecture notes with exercises. Available at*, 2014.

[68] I. Sommerville. *Software Engineering*. Pearson, 9ł edição edition, 2011.

[69] J. L. Szwarcfiter and L. Markenzon. *Estruturas de Dados e seus Algoritmos*, volume 2. Livros Tecnicos e Cientificos, 1994.

[70] S. Thompson. *Type theory and functional programming*. Addison Wesley, 1999.

[71] T. Tsouanas. *Matemática Fundacional para Computação*. http://www.tsouanas.org/fmcbook, Universidade Federal do Rio Grande do Norte, 2017–2021. Work in progress.

[72] D. J. Velleman. *How to prove it: A structured approach*. Cambridge University Press, 2019.

[73] R. Zach, S. Burns, and Z. Qian. *Set Theory: An Open Introduction*. The Open Logic Project, 2021.