Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologias
Engenharia da Computação

Thales L. A. Valente

Disciplina: Linguagens Formais e Autômatos
Código: EECP0020

7 de novembro de 2024

Conteúdo programático

- Elementos de matemática discreta
- Conceitos básicos de linguagens
- Linguagens regulares e autômatos finitos
- Linguagens livres de contexto e autômatos de pilha
- Linguagens sensíveis ao contexto e Máquinas de Turing com fita limitada
- Linguagens recursivas e Máquinas de Turing com finta infinita
- Linguagens recursivamente enumeráveis

Sumário

Definição

- Um **conjunto** pode ser considerado como uma coleção de objetos, chamados de **elementos** ou **membros** do conjunto. Por exemplo, são conjuntos:
  - As vogais a, e, i, o, u.
  - Os dígitos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.
  - Os dias da semana.
  - Os estudantes da UFMA.
  - Os números ímpares $1, 3, 5, 7, \ldots$

Definição

- Para denotar conjuntos, utilizam-se letras maiúsculas. Por exemplo:
  - O conjunto V de vogais.
  - O conjunto D de dias.
  - O conjunto $\mathbb{N}$ dos números naturais.
- Para denotar elementos, utilizam-se letras minúsculas. Por exemplo:
  - x é um elemento de V.
  - y é um elemento de D.
  - z é um elemento de $\mathbb{N}$.
- Para relacionar elementos e conjuntos, utilizam-se as operações de **pertinência**.
  - $x \in V$ quer dizer que o elemento x pertence ao conjunto V.
  - $x \notin V$ quer dizer que o elemento x não pertence ao conjunto V.

Definição

- A ordem dos elementos e a repetição dos mesmo é indiferente para a definição de conjuntos. Por exemplo, os seguintes conjuntos são todos iguais.
  - As vogais a, e, i, o, u.
  - As vogais u, o, i, e, a.
  - As vogais a, i, e, i, o, o, u.
  - As vogais u, u, u, u, o, i, e, a.
- Princípio da extensão: dois conjuntos A e B são iguais se, e somente se, possuírem os mesmo elementos.

Descrição

- Há duas formas de se descrever um conjunto textualmente:
  - Listagem de todos os seus elementos.
    - $V = \{a, e, i, o, u\}$ denota o conjunto V cujos elementos são as letras a, e, i, o, u.
    - Os elementos são separados por vírgula e se encontram entre chaves.
  - Enunciação das propriedades que caracterizam seus elementos.
    - $B = \{x : x\ e\ um\ numero\ par,\ x > 10\}$
    - Os elementos encontram-se entre chaves. Dois pontos significa "tal que". Vírgula significa "e".
    - Lê-se: "*B* é o conjunto dos x tal que x é um número inteiro par e x é maior do que 10."

Conjunto Universo e conjunto Vazio

- O conjunto **Universo** U refere-se àquele ao qual pertencem todos os elementos de uma dada aplicação. Por exemplo:
  - Em geometria plana, o conjunto U representa todos os pontos do plano.
  - Em estudos de populações humanas, o conjunto U representa todas as pessoas.
- O conjunto **Vazio** $\varnothing$ refere-se àquele que não contém elemento algum. Por exemplo:
  - $S = \{x : x \text{ } e \text{ } um \text{ } inteiro \text{ } positivo, \; x^2 = 3\}$

Conjuntos finitos

- **Conjunto finito** é aquele que contém exatamente m elementos distintos, onde m denota algum inteiro não negativo. Por exemplo:
  - O conjunto vazio $\varnothing$ é finito.
  - O conjunto das letras é finito.
  - O conjunto dos números pares é infinito.
- $n(A)$ denota a quantidade de elementos de A.
  - Significa o mesmo que $\#(A)$, $\lceil A \rceil$ ou $card(A)$.

Subconjuntos

- Se todo elemento de um conjunto A é também elemento de um conjunto B, diz-se que A é um **subconjunto** de B. Esse fato é representado por $A \subseteq B$.
- Se A não é subconjunto de B, tem-se que $A \not\subseteq B$.
- Por exemplo:
  - Considere os conjuntos $A = \{1, 3, 4, 5, 8, 9\}$, $B = \{1, 2, 3, 5, 7\}$ e $C = \{1, 5\}$. Então, tem-se que $C \subseteq A$, $C \subseteq B$ e $B \not\subseteq A$.
  - $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
  - Considere os conjuntos $E = \{2, 4, 6\}$ e $F = \{6, 2, 4\}$. Então, tem-se que $E \subseteq F$ e $F \subseteq E$.

Subconjuntos

- Para todo conjunto A, tem-se que $\varnothing \subseteq A \subseteq U$.
- Para todo conjunto A, tem-se que $A \subseteq A$.
- Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.
- Se $A \subseteq B$ e $B \subseteq A$, então $A = B$.

Subconjuntos próprios

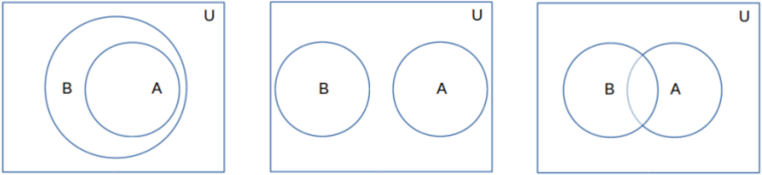
- Um conjunto A é **subconjunto próprio** de B se $A \subseteq B$ mas $A \neq B$. Denota-se este fato por $A \subset B$. Por exemplo:
  - Suponha os conjuntos $A = \{1, 3\}$, $B = \{1, 2, 3\}$ e $C = \{1, 3, 2\}$.
  - Então $A \subset C$ e $B \subseteq C$, pois $B = C$ e $A \neq C$.

Conjunto potência

- O conjunto potência de S, ou as **partes do conjunto** S, refere-se à coleção de todos os subconjuntos de S, denotada por 2^S, ou $Partes(S)$. Note que a $n(2^S)$ é $2^{n(S)}$. Por exemplo, supondo o conjunto $S = \{1, 2, 3\}$, tem-se que:
  - $2^S = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Diagramas de Venn

- Um **diagrama de Venn**[1] é uma representação gráfica na qual os conjuntos são ilustrados por figuras geométricas no plano.
  - Retângulo: representa o conjunto universo U.
  - Círculo: representa qualquer conjunto dentro de U.
- Considerando os conjuntos A e B, tem-se três situações:



(a) $A \subseteq B$

(b) A e B não tem elementos em comum

(c) A e B tem elementos em comum

Figura: Diagramas de Venn

[1] Diagramas de Venn online: `https://www.meta-chart.com/venn`.

Operação de União

- A **união** entre os conjuntos A e B é o conjunto $A \cup B$ de todos os elementos de A e de B. Ou seja, $A \cup B = \{x : x \in A \; ou \; x \in B\}$.
  - Suponha os conjuntos $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$ e $C = \{2, 3, 5, 7\}$.
  - Então $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ e $A \cup C = \{1, 2, 3, 4, 5, 7\}$.

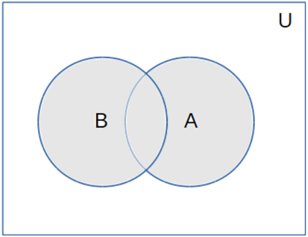


Figura: Diagrama de Venn de $A \cup B$

- Generalização: $A_1 \cup A_2 \cup ... \cup A_m = \cup_{i=1}^{m} A_i = \{x : x \in A_i \; para \; algum \; A_i\}$

Operação de Intersecção

- A **Intersecção** entre os conjuntos A e B é o conjunto $A \cap B$ dos elementos que pertencem simultaneamente a A e a B. Ou seja, $A \cap B = \{x : x \in A \; e \; x \in B\}$.
  - Suponha os conjuntos $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$ e $C = \{2, 3, 5, 7\}$.
  - Então $A \cap B = \{3, 4\}$ e $A \cap C = \{2, 3\}$.

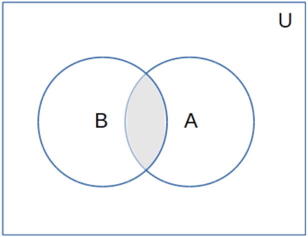
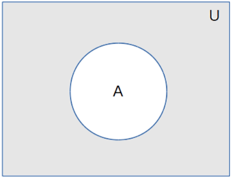


Figura: Diagrama de Venn de $A \cap B$

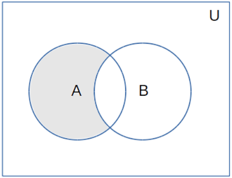
- Generalização: $A_1 \cap A_2 \cap \ldots \cap A_m = \cap_{i=1}^{m} A_i = \{x : x \in A_i \; para \; todo \; A_i\}$

Operações de Complementares

- O **complementar absoluto**, ou simplesmente **complementar**, de um conjunto A, denotado por A^c, é o conjunto dos elementos que pertencem a U mas não a A. Ou seja, $A^c = \{x : x \in U, x \notin A\}$.
- O **complementar relativo** de um conjunto B em relação a A, ou simplesmente a diferença entre A e B, denotado por $A \backslash B$, é o conjunto dos elementos que pertencem a A mas não pertencem a B. Ou seja, $A \backslash B = \{x : x \in A, x \notin B\}$.



(a) A^c está sombreado



(b) $A \backslash B$ está sombreado

Figura: Diagramas de Venn dos complementares

Operação de Diferença simétrica

- A **diferença simétrica** dos conjuntos A e B, denotada por $A \oplus B$, consiste em todos os elementos que pertencem a A ou a B, mas não a ambos. Ou seja, $A \oplus B = (A \cup B) \backslash (A \cap B)$.
  - Suponha os conjuntos $A = \{1, 2, 3, 4, 5, 6\}$ e $B = \{4, 5, 6, 7, 8, 9\}$.
  - Então $A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A \cap B = \{4, 5, 6\}$ e $A \oplus B = \{1, 2, 3, 7, 8, 9\}$.

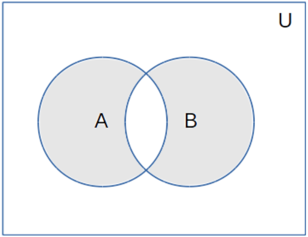


Figura: Diagrama de Venn de $A \oplus B$

Operação de Produto cartesiano

- O **produto cartesiano** dos conjuntos A e B, denotado por $A \times B$, consiste do conjunto de todos os pares ordenados (a, b) com primeira componente em A e segunda componente em B. Ou seja, $A \times B = \{(x, y) : x \in A \text{ e } y \in B\}$.
- Por exemplo, sejam $A = \{1, 2\}$ e $B = \{3, 4\}$, então:
  - $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
  - $B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$
  - $A \times A = A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

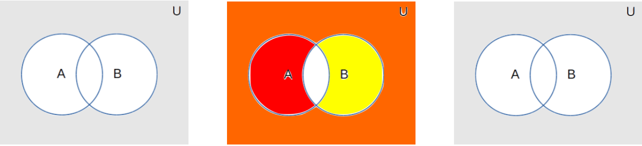
Álgebra de conjuntos

Tabela: Leis da álgebra de conjuntos

Leis de idempotência	(1a) $A \cup A = A$ (1b) $A \cap A = A$
Leis de associatividade	(2a) $(A \cup B) \cup C = A \cup (B \cup C)$ (2b) $(A \cap B) \cap C = A \cap (B \cap C)$
Leis de comutatividade	(3a) $A \cup B = B \cup A$ (3b) $A \cap B = B \cap A$
Leis de distributividade	(4a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (4b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Leis de identidade	(5a) $A \cup \varnothing = A$ (5b) $A \cap U = A$ (6a) $A \cup U = U$ (6b) $A \cap \varnothing = \varnothing$
Leis de involução	(7) $(A^c)^c = A$
Leis dos complementares	(8a) $A \cup A^c = U$ (8b) $A \cap A^c = \varnothing$ (9a) $U^c = \varnothing$ (9b) $\varnothing^c = U$
Leis de DeMorgan	(10a) $(A \cup B)^c = A^c \cap B^c$ (10b) $(A \cap B)^c = A^c \cup B^c$

Álgebra de conjuntos

- Para realizar provas de identidades, recorre-se a duas abordagens:
  - Inclusão em cada direção.
  - Diagrama de Venn.
- Por exemplo, a prova da Lei de DeMorgan $(A \cup B)^c = A^c \cap B^c$:
  - Primeiramente, mostra-se que $(A \cup B)^c \subseteq A^c \cap B^c$.
  - Se $x \in (A \cup B)^c$, então $x \notin (A \cup B)$.
  - Logo, $x \notin A$ e $x \notin B$. Portanto, $x \in A^c$ e $x \in B^c$.
  - Assim, $x \in A^c \cap B^c$.
  - Em seguida, mostra-se $A^c \cap B^c \subseteq (A \cup B)^c$.



(a) $(A \cup B)^c$ (b) $A^c \cap B^c$ (c) $A^c \cap B^c$

Figura: Diagramas de Venn da prova

Sumário

Definição

- Sejam A e B conjuntos. Uma **relação binária R** ou, simplesmente, **relação R** de A para B é um subconjunto de $A \times B$. Portanto, R é o conjunto de pares ordenados onde cada primeiro elemento $a \in A$ e cada segundo elemento $b \in B$. Neste conjunto, cada par (a, b) satisfaz exatamente uma das afirmações seguintes:
  - $(a, b) \in R$, quando dize-se que a é R-relacionado a b, denotado por aRb.
  - $(a, b) \notin R$, quando dize-se que a não é R-relacionado a b, denotado por $a\not{R}b$.
- Por exemplo, sejam os conjuntos $A = \{1, 2, 3\}$, $B = \{x, y, z\}$ e $R = \{(1, y), (1, z), (3, y)\}$. Diz-se que R é uma relação de A para B, pois R é um subconjunto de $A \times B$.

Definição

- Seja R uma relação de um conjunto A para si mesmo, ou seja, R é um subconjunto de $A^2 = A \times A$. Então diz-se que ***R* é uma relação em *A***.
- O **domínio** de uma relação R é o conjunto de todos os primeiros elementos dos pares ordenados de R.
- A **imagem** de uma relação R é o conjunto de todos os segundos elementos dos pares ordenados de R.
- A **inversa** de uma relação R de A para B consiste na relação R^{-1}, cujos pares ordenados, quando invertidos, pertencem a R. Assim, tem-se que:

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

Definição

- Por exemplo, sejam os conjuntos $A = \{1, 2, 3\}$, $B = \{x, y, z\}$ e $R = \{(1, y), (1, z), (3, y)\}$. Tem-se:
  - O domínio de R é $\{1, 3\}$.
  - A imagem de R é $\{y, z\}$.
  - A inversa de R é $\{(y, 1), (z, 1), (y, 3)\}$.

Tipos de relações

- Dado um conjunto A, alguns tipos básicos de relação podem ser definidos em A, a saber:
  - Reflexivas
  - Simétricas
  - Transitivas

Tipos de relações

- Uma relação R em um conjunto A é **reflexiva** se aRa acontece para todo $a \in A$, isto é, se $(a, a) \in R$ para todo $a \in A$.
- Por exemplo, quais dos itens abaixo representam relações reflexivas?
    1. Relação $\leq$ (menor que) no conjunto $\mathbb{Z}$.
    2. Inclusão de conjuntos $\subseteq$ em uma coleção C de conjuntos.
    3. Relação $\perp$ (perpendicularidade) em um conjunto L de retas no plano.
    4. Relação $\parallel$ (paralelismo) em um conjunto L de retas no plano.
    5. Relação $|$ de divisibilidade no conjunto $\mathbb{N}$.

Tipos de relações

- Uma relação R em um conjunto A é **simétrica** se aRb implica bRa, isto é, se $(a, b) \in R$ implica $(b, a) \in R$.
- Por exemplo, quais dos itens abaixo representam relações simétricas?
  1. $R_1 = \{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\}$;
  2. $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$;
  3. $R_3 = \{(1, 3), (2, 1)\}$;
  4. $R_4 = \varnothing$, a relação vazia;
  5. $R_5 = A \times A$, a relação universal.

Tipos de relações

- Uma relação R em um conjunto A é **transitiva** se aRb e bRc implica aRc, isto é, se (a, b) e $(b, c) \in R$, então $(a, c) \in R$.
- Por exemplo, quais dos itens abaixo representam relações transitivas?
  1. $R_1 = \{(1, 1), (1, 2), (2, 3), (1, 3), (4, 4)\}$;
  2. $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$;
  3. $R_3 = \{(1, 3), (2, 1)\}$;
  4. $R_4 = \varnothing$, a relação vazia;
  5. $R_5 = A \times A$, a relação universal.

Relações de equivalência

- Uma relação R em um conjunto não vazio S é uma **relação de equivalência** se R é reflexiva, simétrica e transitiva. Isto é, R é uma relação de equivalência em S se possui as seguintes propriedades:
  - Para todo $a \in A$, aRa.
  - Se aRb, então bRa.
  - Se aRb e bRc, então aRc.
- Por exemplo, são relações de equivalência:
  - A classificação de animais em espécies, isto é, a relação "é da mesma espécie que", definida no conjunto de animais.
  - A relação $\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$, definida no conjunto $\{1,2,3\}$.
  - A relação "$x+y$ é par", definida no conjunto $\mathbb{N}$.
  - A relação "$x=y^2$", definida no conjunto $\{0,1\}$.

Sumário

- Conjuntos
- Relações
- Funções
- Teoremas e demonstrações
- Grafos
- Árvores

Definição

- Uma **função** $\boldsymbol{f}$ de um conjunto A em um conjunto B é definida como a coleção de associações entre cada elemento de A e um único elemento de B. Simbolicamente, tem-se:
  - $f : A \to B$, lido como "f é uma função de A em B".
  - A é dito o **domínio** de f.
  - B é dito o **contradomínio** de f.
  - Se $a \in A$, então $f(a)$ é chamada de imagem de a por f. Ao conjunto de todos os $f(a)$ dá-se o nome de **imagem** de f. Em termos simples, a imagem é o conjunto de todos os resultados possíveis da função f.
- No exemplo $f(x) = x^2$, sendo o domínio de $f = (x)$

Definição

- Por exemplo, tem-se as seguintes funções:
  - $f(x) = x^2$ é a função que associa a cada número real o seu quadrado.
  - f é a função que associa a cada país do mundo sua capital.
  - 1_A é a função **Identidade**, que associa cada elemento do domínio A a si mesmo.
  - f de $A = \{a, b, c, d\}$ em $B = \{r, s, t, u\}$, como definida pela figura abaixo.

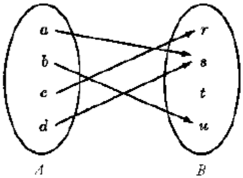


Figura: Função $f : A \rightarrow B$

Definição

- De um outro ponto de vista, uma função $f : A \to B$ é uma **relação** de A para B (ou seja, um subconjunto de $A \times B$) tal que cada $a \in A$ pertence à primeira posição de um único par ordenado (a, b) em f. Assim, tem-se que o **gráfico** de f pode ser definido por

$$\text{Gráfico de } f = \{(a, b) : a \in A, b = f(a)\}$$

- Por exemplo, dadas as relações abaixo, pode-se verificar quais são funções no conjunto $A = \{1, 2, 3\}$.
  - $f = \{(1, 3), (2, 3), (3, 1)\}$ é função de A em A, pois cada elemento de A aparece uma única vez como primeiro elemento de um par ordenado em f.
  - $g = \{(1, 2), (3, 1)\}$ não é função pois $2 \in A$ não aparece em um par ordenado em f.
  - $h = \{(1, 3), (2, 1), (1, 2), (3, 1)\}$ não é função pois $1 \in A$ aparece como primeiro elemento em mais de um par ordenado em f.

Injetividade, sobrejetividade e bijetividade

- Uma função $f : A \to B$ é dita **injetora** se elementos diferentes do domínio A tem imagens distintas, ou seja, f é injetora se $f(a) = f(a')$ implica $a = a'$.
- Uma função $f : A \to B$ é dita **sobrejetora** se cada elemento de B é a imagem de algum elemento de A, ou seja, f é sobrejetora se a imagem de f é todo contradomínio B de f.
- Uma função $f : A \to B$ é dita **bijetora** se ela for simultaneamente injetora e sobrejetora.

Injetividade, sobrejetividade e bijetividade

- Por exemplo, considere as funções $f_1 : A \to B$, $f_2 : B \to C$, $f_3 : C \to D$ e $f_4 : D \to E$ ilustradas pelos diagramas abaixo:

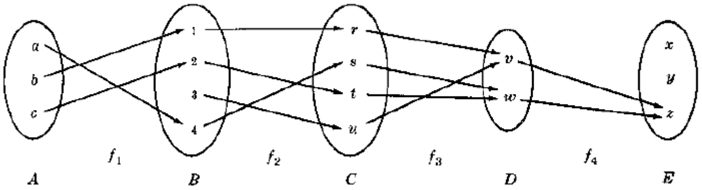


Figura: Função $f : A \to B$

- As funções possuem as seguintes características:
  - f_1 é injetora mas não sobrejetora.
  - f_2 é injetora e sobrejetora.
  - f_3 não é injetora mas é sobrejetora.
  - f_4 não é injetora nem sobrejetora.

Sumário

Tipos de demonstrações

- Linguagens Formais e Autômatos são sistemas matemáticos formais. Como tais, possuem inúmeras propriedades que necessitam ser provadas.
- As propriedades geralmente formuladas como teoremas. Um **teorema** é uma afirmação que pode ser demonstrada verdadeira através de operações e argumentos matemáticos.
- A **demonstração** de um teorema exige a prova formal de que uma certa propriedade é satisfeita por todos os membros de um conjunto. Dentre as técnicas utilizadas para tanto, destacam-se as seguinte:
  - Demonstrações por indução matemática.
  - Provas por contradição.

Indução matemática

- Imagine que você esteja subindo uma escada infinitamente alta. Pergunta-se: como você sabe se será capaz de chegar a um degrau arbitrariamente alto?

Indução matemática

- Pode-se fazer as seguintes hipóteses sobre sua capacidade de subida de escada:
    - Você consegue alcançar o primeiro degrau.
    - Uma vez chegando a um degrau, você é sempre capaz de chegar ao próximo.
- Se ambas as hipóteses forem verdadeiras, pode-se subir tão alto quanto se queira.
- Esta forma de raciocínio que leva à conclusão de um certo caso com base na observação da regularidade de uma ocorrência é chamada de **indução**.

Indução matemática

- **Primeiro princípio de indução matemática:** Seja P uma propriedade definida nos inteiros positivos $\mathbb{N} = \{1, 2, 3, ...\}$, i.e., $P(k)$ é verdadeiro ou falso para cada k em $\mathbb{N}$. Suponha que P tenha as seguintes propriedades:
  1. $P(1)$ é verdadeiro.
  2. $P(k+1)$ é verdadeiro sempre que $P(k)$ for verdadeiro.

  Então, P é verdade para todo inteiro positivo.
- Neste caso, tem-se as seguintes denominações:
  - base da indução: $P(1)$.
  - hipótese da indução: $P(k)$.
  - passo da indução: $P(k)$ implica em $P(k+1)$.

Indução matemática

- **Exemplo 1**: prove que a equação $1 + 3 + 5 + ... + (2n - 1) = n^2$ é verdadeira para qualquer inteiro positivo n.
  - Etapas da prova indutiva:
    1. **Prove a base da indução $P(1)$.**
       $1 = 1^2$ é verdade.
    2. **Suponha $P(k)$.**
       $1 + 3 + 5 + ... + (2k - 1) = k^2$
    3. **Prove $P(k + 1)$.**
       $1 + 3 + 5 + ... + [2(k + 1) - 1] \stackrel{?}{=} (k + 1)^2$

$$\begin{aligned} & 1 + 3 + 5 + ... + [2(k+1) - 1] \\ & = 1 + 3 + 5 + ... + (2k - 1) + [2(k + 1) - 1] \\ & = k^2 + [2(k + 1) - 1] \\ & = k^2 + [2k + 2 - 1] \\ & = k^2 + 2k + 1 \\ & = (k + 1)^2 \end{aligned}$$

Indução matemática

- **Exemplo 2**: prove que, para qualquer inteiro positivo n a equação $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$ é verdadeira.
  - Etapas da prova indutiva:
    1. **Prove a base da indução.** $1 = \frac{1(1+1)}{2} = 1$
    2. **Suponha $P(k)$.**
       $1 + 2 + 3 + ... + k = \frac{k(k+1)}{2}$
    3. **Prove $P(k+1)$.**
       $1 + 2 + 3 + ... + k + 1 \stackrel{?}{=} \frac{(k+1)(k+1+1)}{2} = 1 + 2 + 3 + ... + k + k + 1$

$$
\begin{aligned}
&= \frac{k(k+1)}{2} + k + 1 \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}
$$

Prova por contradição

- A **prova por contradição** ou **redução ao absurdo** consiste em adotar como base da demonstração a negação da hipótese formulada e, através de manipulações lógicas, mostrar que q negação dessa hipótese conduz a uma contradição.

Prova por contradição

- **Exemplo 1**: prove, por contradição, que $\sqrt{2}$ é um número irracional.
  - Inicialmente, suponha a negação da hipótese, ou seja, que $\sqrt{2}$ é um número racional.
  - Sob a suposição de racionalidade, $\sqrt{2}$ pode ser expresso como $\sqrt{2} = \frac{p}{q}$, com p e q números inteiros sem fatores comuns.
  - Manipulando $\sqrt{2} = \frac{p}{q}$, tem-se $p^2 = 2q^2$. Assim, p^2 e, consequentemente, p são números pares.
  - Sendo par, p pode ser escrito como $p = 2m$. Substituindo na equação acima, tem-se $q^2 = 2m^2$. Portanto, q^2 e q também são pares.
  - Se p e q são pares, então eles possuem 2 como fator comum. Mas isso contradiz a suposição inicial de que não haveria fatores comuns entre p e q. Conclui-se, portanto, que a suposição inicial está errada e que $\sqrt{2}$ tem que ser um número irracional.

Prova por contradição

- **Exemplo 2**: prove, por contradição, que 0 é o único elemento neutro da adição em $\mathbb{N}$.
  - Inicialmente, suponha a negação da hipótese, ou seja, que 0 não é o único elemento neutro da adição em $\mathbb{N}$.
  - Sob essa suposição, deve existe um número $e \in \mathbb{N}$, tal que $e \neq 0$.
  - Como 0 é elemento neutro, tem-se, para qualquer número $n \in \mathbb{N}$, que $n = n + 0$. Em particular, para $n = e$, tem-se que $e = e + 0$.
  - Como e é elemento neutro, tem-se, para qualquer número $n \in \mathbb{N}$, que $n = e + n$. Em particular, para $n = 0$, tem-se que $0 = e + 0$.
  - Como $e = e + 0$ e $0 = e + 0$, então $e = 0$. Mas isso contradiz a suposição inicial de que $e \neq 0$. Conlui-se, portanto, que a suposição inicial está errada e que 0 tem de ser o único elemento neutro da adição em $\mathbb{N}$.

Sumário

- Conjuntos
- Relações
- Funções
- Teoremas e demonstrações
- Grafos
- Árvores

Definição

- Um **grafo** é um par ordenado (V, A), em que V denota o conjunto de **vértices** (ou nós) do grafo e A denota a relação binária sobre V, através do qual são especificados os **arcos** do grafo.
  - Dois vértices $v_i, v_j \in V$ tais que $(v_i, v_j) \in A$ são ditos adjacentes.
- Abaixo, tem-se o grafo G_1, representando textualmente e graficamente.

$G_1 = (V_1, A_1)$
$V_1 = \{0, 1, 2, 3\}$
$A_1 = \{(0, 1), (0, 2), (0, 3), (1, 3), (2, 3)\}$

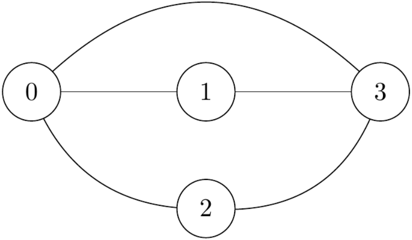


Figura: Grafo G_1

Definição

- Um grafo **orientado** é aquele em que há uma relação de ordem entre os elementos que formam os pares $(v_i, v_j) \in A$. Caso contrário, o grafo é dito **não-orientado**.
  - No caso de $(v_i, v_j) \in A$, diz-se que v_i é o predecessor de v_j e v_j é o sucessor de v_i.
- Abaixo, tem-se o grafo orientado G_2.

$$G_2 = (V_2, A_2)$$
$$V_2 = \{0, 1, 2, 3\}$$
$$A_2 = \{(0,1), (0,2), (0,3), (1,3), (2,3)\}$$

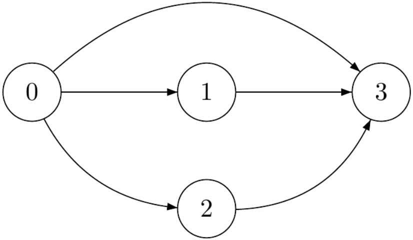


Figura: Grafo G_2

Definição

- Um grafo é dito **ordenado** quando houver uma relação de ordem pré-convencionada sobre todos os arcos que emergem dos diversos vértices do grafo.
- Por exemplo, abaixo tem-se o grafo G_3:
  $G_3 = (V_3, A_3)$
  $V_3 = \{a, b, c, d\}$
  $A_3 = \{(a, b), (b, a), (a, c), (a, d), (c, b), (d, c), (c, d)\}$

  Suponha que exista uma relação de ordem implícita entre os pares ordenados de A_3 de tal forma que $(a, b) < (b, a) < (a, c) < (a, d) < (c, b) < (d, c) < (c, d)$. Então, tem-se que:

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

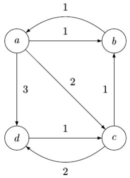


Figura: Grafo G_3

Definição

- Os seguinte conceitos valem para grafos orientados:
  - **Ramificação de saída (N_S)**: quantidade de arcos que partem de um dado vértice.
  - **Ramificação de entrada (N_E)**: quantidade de arcos que chegam a um dado vértice.
  - **Vértices-base ou vértices-raiz**: vértices com $N_E = 0$.
  - **Vértices-folha**: vértices com $N_S = 0$.
- Por exemplo, tem-se, para o grafo G_3 definido anteriormente:

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

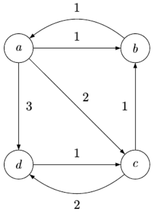


Figura: Grafo G_3

Definição

- Os seguintes conceitos valem para grafos:
    - O **caminho** entre dois vértices **inicial** e **final** é a sequência ordenada de arcos tal que predecessor do primeiro arco é o vértice inicial, o sucessor do último arco é o vértice final e cada arco intermediário tem como predecessor o sucessor do arco anterior.
    - Um **ciclo** é um caminho cujo predecessor do primeiro arco e o sucessor do último arco coincidem. Grafos que apresentam ao menos um ciclo são ditos **cíclicos**. Grafos sem ciclos são **acíclicos**.
    - O **comprimento** do caminho é o número de arcos que o formam.
- Por exemplo, tem-se que, para o grafo G_3 definido anteriormente:
    - A seqüência $(a, c)(c, b)$ constitui um caminho de comprimento 2.
    - A seqüência $(a, d)(c, d)(d, c)$ não constitui um caminho.
    - O grafo G_3 é do tipo cíclico.

Definição

- Um grafo **rotulado** é aquele que, associado a seus vértices ou a seus arcos, há rótulos que representam informação adicional.
    - Uma **rotulação de vértices** (**de arcos**)é uma função f_V (uma função f_A) que associa os elementos de V (de A) a elementos de um conjunto R_V (de um conjunto R_A), chamado de alfabeto de rotuação de vértices (de arcos).
- Por exemplo, seja o grafo G_4 abaixo:
  $G_4 = (V_4, A_4)$
  $V_4 = \{0, 1, 2\}$
  $A_4 = \{(0, 1), (1, 2), (0, 2)\}$

  Uma rotulação possível seria:

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

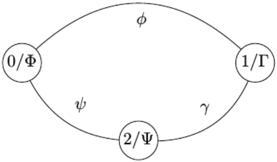


Figura: Grafo G_3

Sumário

- Conjuntos
- Relações
- Funções
- Teoremas e demonstrações
- Grafos
- Árvores

Definição

- Um **árvore** é um grafo acíclico orientado e ordenado que possui as seguintes características adicionais:
  - Há apenas um vértice r tal que $N_E(r) = 0$. Ele é chamado de **raiz**.
  - Todos os demais vértices possuem $N_E = 1$.
  - Para cada vértice, há sempre um único caminho que o liga à raiz da árvore.

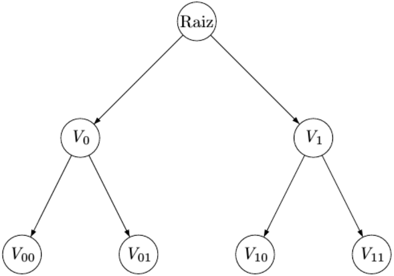


Figura: Árvore

Definição

- Os seguintes conceitos valem para árvores:
  - Para vértices a e b que fazem parte de um mesmo caminho em uma árvore, diz-se que a é **ancestral** de b se for possível atingir b a partir de a. Nesse caso, b é dito **descendente** de a.
  - Quando entre a e b não houver nenhum vértice intermediário, diz-se que a e b são **adjacentes**.
  - Quando a é ancestral direto de b, diz-se a é **pai** de b e b é **filho** de a.
  - Vértices sem filhos são chamandos de **folhas** e os demais vértices **internos**.
  - A **profundidade** de um nó é o comprimento do caminho entre a raiz e esse nó.

Definição

- Por exemplo, considerando a árvore abaixo, são verdadeiras as afirmações que seguem:

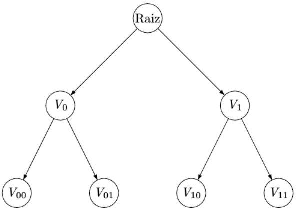


Figura: Árvore

- V_1 é pai de V_{11} e V_{11} é filho de V_1.
- *Raiz* é ancestral de V_{00}.
- V_{01} é descendente de *Raiz*.
- V_{00} e V_{11} são folhas da árvore.
- V_0 e V_1 são nós internos da árvore.
- V_{01} e V_{10} possuem profundidade 2.

Bibliografia

1. RAMOS, Marcus V. M. Linguagens formais: teoria, modelagem e implementação. 1ª ed. Porto Alegre: Bookman, 2009.
    - **Capítulo 1**.

Dúvidas?