Capítulo 1: Conceitos Preliminares

Newton José Vieira

Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

17 de março de 2011

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

Sumário

A matemática entre a entidade e a representação

Entidade	*Modelo matemático*	*Representação*
mês	número inteiro no intervalo $[1, 12]$	um dos caracteres 0 a 9, A ou B
remuneração	número real positivo	base 10
presença	vetor de números, um para cada dia do mês	sequência de reais na base 10
FP	relação	"arquivo"
cálculo de FP	algoritmo	programa

Sequência de símbolos: elemento fundamental das **linguagens formais**.

Características de provas de teoremas

- Estilo:
  - formal $\times$ informal;
  - conciso $\times$ prolixo.
- Prova:
  - vocabulário limitado: **se** . . . **então**, **contradição** etc;
  - usa técnicas de prova.

Representação
Prova de Teoremas
Conjuntos
Relações
Funções
Conjuntos Enumeráveis
Definições Recursivas
Indução Matemática
Grafos
Linguagens Formais
Gramáticas
Problemas de Decisão

Conectivos lógicos

Os conectivos lógicos: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$, $\forall$, $\exists$.

Tabela da verdade para a negação

Negação

α	$\neg\alpha$
V	F
F	V

Newton José Vieira Capítulo 1: Conceitos Preliminares

Conectivos lógicos

Tabela da verdade para a conjunção

Conjunção

α	β	$\alpha \wedge \beta$
V	V	V
V	F	F
F	V	F
F	F	F

Conectivos lógicos

Tabela da verdade para a disjunção

Disjunção

α	β	$\alpha \vee \beta$
V	V	V
V	F	V
F	V	V
F	F	F

Conectivos lógicos

Tabela da verdade para a condicional

Condicional

α	β	$\alpha \rightarrow \beta$
V	V	V
V	F	F
F	V	V
F	F	V

Conectivos lógicos

Tabela da verdade para a bicondicional

Bicondicional

α	β	$\alpha \leftrightarrow \beta$
V	V	V
V	F	F
F	V	F
F	F	V

Quantificação

- **Quantificação universal:** $\forall x P(x)$
  P(x) é verdadeira
  para todo x do universo.
- **Quantificação existencial:** $\exists x P(x)$
  P(x) é verdadeira
  para algum x do universo.

Exemplo:

Expressar formalmente:
todo número natural par ao quadrado é par.

Afirmativa válida

Verdadeira para todos os valores-verdade de suas subafirmativas.
Exemplos:

- $\alpha \vee \neg\alpha$
- $\alpha \rightarrow \alpha$
- $\alpha \vee (\alpha \rightarrow \beta)$
- $P(a) \rightarrow \exists x P(x)$
- $\forall x P(x) \leftrightarrow \neg\exists x \neg P(x)$

Contradição

Falsa para todos os valores-verdade de suas subafirmativas.
Exemplos:

- $\alpha \wedge \neg\alpha$
- $\alpha \leftrightarrow \neg\alpha$
- $(\alpha \wedge (\alpha \rightarrow \beta)) \wedge \neg\beta$
- $P(a) \wedge \neg\exists x P(x)$
- $\forall x P(x) \wedge \exists x \neg P(x)$

Equivalência lógica

$\alpha \equiv \beta$ se o valor-verdade de α e β é o mesmo para todos os valores-verdade de suas subafirmativas.
Exemplos:

- $\alpha \vee \beta \equiv \beta \vee \alpha$
- $\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
- $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
- $\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$
- $\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\alpha \rightarrow \beta)$
- $\neg\forall x P(x) \equiv \exists x \neg P(x)$

Consequência lógica (implicação lógica)

$\Gamma \Rightarrow \beta$ se β é verdadeira sempre que as afirmativas em Γ também são.

Exemplos:

- $\{\alpha \to \beta, \alpha\} \Rightarrow \beta$
- $\{\alpha \to \beta, \neg\beta\} \Rightarrow \neg\alpha$
- $\{\alpha \to \beta, \neg\alpha \to \beta\} \Rightarrow \beta$
- $\{\alpha \to \beta, \beta \to \gamma\} \Rightarrow \alpha \to \gamma$
- $\{P(a) \Rightarrow \exists x P(x)$
- $\{P(a), \forall x(P(x) \to Q(x))\} \Rightarrow Q(a)$

Exemplos de **regras de inferência**

$$\begin{array}{l}\alpha\\ \alpha \to \beta\\ \hline \beta\end{array} \qquad \begin{array}{l}\alpha\\ \neg\alpha \vee \beta\\ \hline \beta\end{array} \qquad \begin{array}{l}\neg\beta\\ \alpha \to \beta\\ \hline \neg\alpha\end{array}$$

$$\begin{array}{l}\alpha \to \beta\\ \neg\alpha \to \beta\\ \hline \beta\end{array} \qquad \begin{array}{l}\alpha \to \beta\\ \beta \to \gamma\\ \hline \alpha \to \gamma\end{array} \qquad \begin{array}{l}\alpha \leftrightarrow \beta\\ \beta \leftrightarrow \gamma\\ \hline \alpha \leftrightarrow \gamma\end{array}$$

Relação entre $\to$ e $\Rightarrow$:

se $\Gamma \cup \{\alpha\} \Rightarrow \beta$, então $\Gamma \Rightarrow \alpha \to \beta$.

Técnica de prova: direta

Prova direta da implicação

Para provar $\alpha \to \beta$:

1. Supor α.
2. Provar β.

Exemplo:

- n é par $\to$ n^2 é par.

Técnica de prova: pela contrapositiva

Prova da implicação pela contrapositiva

Para provar $\alpha \to \beta$:

1. Supor $\neg\beta$.
2. Provar $\neg\alpha$.

Exemplo:

- n^2 é par $\to$ n é par.

Técnica de prova: para universal

Prova de uma universal

Para provar $\forall x P(x)$:

1. Supor um x arbitrário (que não ocorre ainda).
2. Provar $P(x)$.

Exemplo:

- $\forall n \in \mathbf{N}(n \text{ é par } \rightarrow n^2 \text{ é par})$.

Técnica de prova: por contradição

Prova de uma afirmativa por contradição

Para provar α:

1. Supor $\neg\alpha$.
2. Provar uma contradição.

Exemplo:

- Existe uma infinidade de números primos.

Técnica de prova: por construção

Prova de uma existencial por construção

Para provar $\exists x \in A P(x)$:

1. Encontrar um $a \in A$ tal que $P(a)$.
2. Provar $P(a)$.

Exemplo:

- $\forall n \in \mathbf{N} \exists k \in \mathbf{N}$ k tem n divisores distintos.

Técnica de prova: por casos

Prova de uma afirmativa por casos

Para provar β:

1. Provar $\alpha_1 \vee \ldots \vee \alpha_n$.
2. Provar $\alpha_1 \rightarrow \beta, \ldots, \alpha_n \rightarrow \beta$.

Exemplo:

- $\forall x, y \in \mathbf{R}\ min(x, y) + max(x, y) = x + y$.

Técnica de prova: para bicondicional

Prova de uma bicondicional em duas partes

Para provar $\alpha \leftrightarrow \beta$:

1. Provar $\alpha \rightarrow \beta$.
2. Provar $\beta \rightarrow \alpha$.

Exemplo:

- $\forall n \in \mathbf{N}$ (n par $\leftrightarrow$ n^2 par).

O que é um conjunto?

Abstração matemática que visa capturar o conceito de coleção.
Lista não ordenada de **elementos** ou **membros**: $\{1, 2\} = \{2, 1\}$
Notação:

- $a \in A$: a **pertence** a A.
- $a \notin A$: a não pertence a A.

Exemplos:

- $\{Mercúrio, Vênus, Terra, Marte, Júpiter\}$
- $\{10, Marte, \{0\}, \{Terra, 1, 2, 3\}\}$

Tipos de conjuntos e conjuntos importantes

- O **conjunto vazio**: $\emptyset$.
- Conjuntos **unitário**, **finito**, **infinito**.
- **N**: números **naturais**.
- **Z**: números **inteiros**.
- **R**: números **reais**.
- **Q**: números **racionais**.

Notações importantes:

$\{x \mid P(x)\}$. Exemplo: $\{k \mid k = 2n + 1 \text{ e } n \in \mathbf{N}\}$.
$\{x \in A \mid P(x)\}$. Exemplo: $\{k \in \mathbf{R} \mid 0 \leq k \leq 1\}$.

Relações entre conjuntos

Relações básicas entre conjuntos

- **Suconjunto:** $A \subseteq B$ se e somente se $\forall x(x \in A \rightarrow x \in B)$.
- **Suconjunto próprio:** $A \subset B$ se e somente se $A \subseteq B$ e $A \neq B$.

Exemplos:

- $\emptyset \subseteq A$
- $\emptyset \subset A$ se $A \neq \emptyset$
- $\emptyset \not\subset \emptyset$

Operações sobre conjuntos

Operações básicas sobre conjuntos

- **União:** $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$.
- **Interseção:** $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$.
- **Diferença:** $A - B = \{x \mid x \in A \text{ e } x \notin B\}$.
- **Complemento:** $\overline{A} = U - A$.

Exemplos de identidades

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$
$$A - B = A \cap \overline{B}$$

Igualdade

$A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$.

Prova de igualdade de conjuntos

Para provar $A = B$:

1. Provar $A \subseteq B$.
2. Provar $B \subseteq A$.

Algumas vezes é possível provar encadeando-se $\leftrightarrow$s.

Exemplo:

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

Conjuntos disjuntos

A e B são **disjuntos** se e somente se $A \cap B = \emptyset$.

Exemplos:

- $\{0, 2, 4\}$ e $\{1, 3, 5\}$
- $\emptyset$ e A.
- A e $\overline{A}$.
- $A - B$ e $B - A$.

União e interseção generalizadas

União de n conjuntos

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n.$$

Interseção de n conjuntos

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n.$$

Partição

Partição de um conjunto

Uma **partição** de A é o conjunto $\{B_1, \ldots, B_n\}$ tal que:

1. $B_i \neq \emptyset$ para $1 \leq i \leq n$;
2. $B_i \cap B_j = \emptyset$ para $1 \leq i < j \leq n$; e
3. $\bigcup_{i=1}^{n} B_i = A$.

Exemplo: quais são as partições de $\{1, 2, 3\}$?

Conjunto potência; número de elementos

Conjunto potência

Conjunto potência de A: $\mathcal{P}(A) = \{X \mid X \subseteq A\}$.

Exemplo: que conjunto é $\mathcal{P}(\{1, 2, 3\})$?

Notação para **número de elementos** de A: $|A|$.
Exemplos: $|\emptyset| = 0$, $|\{\emptyset, 1, 2, \{1, 2, 3, 4, 5\}\}| = 4$, $|\mathcal{P}(A)| = 2^{|A|}$.

Produto cartesiano

Par não ordenado: (a, b) ou $[a, b]$.
Similarmente: tripla, quádrupla etc.

Produto cartesiano de dois conjuntos

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

Exemplos:

- $\emptyset \times \{1, 2\} = \emptyset$.
- $\{1, 2\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.
- $|A \times B| = |A|.|B|$ se A e B forem finitos.

Produto cartesiano de n conjuntos: A^n.

O que é relação

Relação de n argumentos sobre $A_1, \ldots, A_n$

Um subconjunto de $A_1 \times A_2 \times \ldots \times A_n$.

Relação **binária**: $R \subseteq A \times B$

Domínio: A.

Contradomínio: B.

Imagem: $\{y \mid (x, y) \in R \text{ para algum } x\}$.

Notação: $(x, y) \in R$ é o mesmo que $x\,R\,y$.

Representação
Prova de Teoremas
Conjuntos
Relações
Funções
Conjuntos Enumeráveis
Definições Recursivas
Indução Matemática
Grafos
Linguagens Formais
Gramáticas
Problemas de Decisão

Um exemplo de reação binária

Relação $< \subseteq \mathbf{N} \times \mathbf{N}$:

- domínio: $\mathbf{N}$;
- contradomínio: $\mathbf{N} - \{0\}$;
- imagem: $\mathbf{N} - \{0\}$.

Newton José Vieira Capítulo 1: Conceitos Preliminares

Representação
Prova de Teoremas
Conjuntos
Relações
Funções
Conjuntos Enumeráveis
Definições Recursivas
Indução Matemática
Grafos
Linguagens Formais
Gramáticas
Problemas de Decisão

Propriedades

Inversa de R

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

Propriedades de uma relação binária $R \subseteq A \times A$

- **Reflexiva**: $\forall x \in A\,[xRx]$
- **Simétrica**: $\forall x, y \in A\,[xRy \to yRx]$.
- **Transitiva**: $\forall x, y, z \in A\,[(xRy \wedge yRz) \to xRz]$.

Newton José Vieira Capítulo 1: Conceitos Preliminares

Representação
Prova de Teoremas
Conjuntos
Relações
Funções
Conjuntos Enumeráveis
Definições Recursivas
Indução Matemática
Grafos
Linguagens Formais
Gramáticas
Problemas de Decisão

Propriedades/exemplos

Considere as relações:

- $<$ sobre $\mathbf{N}$;
- $\leq$ sobre $\mathbf{N}$;
- $\subseteq$ sobre $\mathcal{P}(\mathbf{N})$;
- $\equiv$ sobre o conjunto das afirmativas da lógica proposicional.

Para cada uma diga se a mesma é reflexiva, simétrica e transitiva.

Newton José Vieira Capítulo 1: Conceitos Preliminares

Relação de equivalência

Relação de equivalência

Aquela que é reflexiva, simétrica e transitiva.

$\Longrightarrow$Induz **classes de equivalência**.

Exemplos:

- $(mod\ \ n) = \{(x, y) \in \mathbf{N}^2 \mid x\ mod\ n = y\ mod\ n\}$
- *fazem aniversário no mesmo dia*.

Que classes de equivalência induz (mod 2)? E (mod 10)?
E "*fazem aniversário no mesmo dia*"?

Fechos de uma relação

Fecho reflexivo

O **Fecho reflexivo** de $R \subseteq A \times A$ é S tal que:

- $R \subseteq S$;
- S é reflexiva;
- se $R \subseteq T$ e T é reflexiva, $S \subseteq T$.

Fechos **simétrico** e **transitivo**: análogos.

Qual é o fecho reflexivo de $<$? Qual é o fecho simétrico de $<$?

O que é uma função

Função parcial

Uma **função** $f : A \rightarrow B$: é uma relação $f \subseteq A \times B$ tal que:

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

- $(x, y) \in f$ é o mesmo que $f(x) = y$.
- f é **indefinida** para x se não há y tal que $f(x) = y$.
- Função **total**: definida para todo argumento.
- Função $f : A \rightarrow B$ de n argumentos:
  $A = A_1 \times \ldots \times A_n$.

Exemplos de funções

- $+ : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ (total)
- $/ : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ (parcial)

Composição de funções

Composição: $g \circ f(x) = g(f(x))$.
Exemplo:
Sejam $f : \mathbf{Z} \to \mathbf{N}$ tal que $f(n) = |n| + 1$
$g : \mathbf{N} \to \mathbf{Z}$ tal que $g(n) = 1 - n$.
Então:

- $g \circ f : \mathbf{Z} \to \mathbf{Z}$ é tal que
  $(g \circ f)(n) = g(f(n)) = g(|n| + 1) = 1 - (|n| + 1) = -|n|$.
- $f \circ g : \mathbf{N} \to \mathbf{N}$ é tal que
  $(f \circ g)(n) = f(g(n)) = f(1 - n) = |1 - n| + 1$.

Tipos de funções

Uma função total $f : A \to B$ é:

- **Injetora**: se $\forall x, y\, [x \neq y \to f(x) \neq f(y)]$.
  Ex: $f : \mathbf{N} \to \mathbf{N}$ tal que $f(n) = 2n$.
- **Sobrejetora**: se B é a imagem de f.
  Ex: $g : \mathbf{Z} \to \mathbf{N}$ tal que $g(n) = |n|$.
- **Bijetora**: se é injetora e sobrejetora.
  Ex: $h : \mathbf{Z} \to \mathbf{N}$ tal que $h(n) = 2n$ se $n \geq 0$, e $h(n) = -(2n + 1)$ se $n < 0$.

O que é conjunto enumerável

Cardinalidade

$card(A) = card(B)$ se existe uma função bijetora de A para B.

$\Longrightarrow$ $card(A) = card(B)$ se $|A| = |B|$, caso A e B sejam finitos.
$\Longrightarrow$ A é **infinito** se existe $X \subset A$ tal que $card(X) = card(A)$.

Conjunto enumerável

A é **enumerável** se $card\ (A) = card\ (\mathbf{N})$.

Conjunto **contável**: finito ou enumerável.

Um exemplo de conjunto enumerável

O conjunto $\mathbf{Z}$ é enumerável:

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & \cdots \end{array}$$

Um teorema facilitador

As seguintes afirmativas são equivalentes:

1. A é contável.
2. Existe função injetora de A para $\mathbf{N}$.
3. $A = \emptyset$ ou existe função sobrejetora de $\mathbf{N}$ para A.

Mais um exemplo de conjunto enumerável

O conjunto dos racionais positivos, QP, é enumerável:

	1	2	3	4	5	$\cdots$
0	0	1	3	6	10	
1	2	4	7	11		
2	5	8	12			
3	9	13				
4	14					
$\vdots$						

$f(i,j) = (i+j)(i+j-1)/2 + i$ é bijetora. Logo, existe uma função sobrejetora de $\mathbf{N}$ para QP!

Resultados importantes

1. Todo subconjunto de conjunto contável é contável.
2. $A \times B$ é contável se A e B são contáveis.
3. $A \cup B$ é contável se A e B são contáveis.

Provando que um conjunto não é contável

Para provar que um conjunto infinito não é enumerável:

usar o método da **diagonalização de Cantor**.

$\mathcal{P}(\mathbf{N})$ não é enumerável:

	0	1	2	3	$\cdots$
C_0	$\boxed{\in \text{ ou } \notin}$	$\in$ ou $\notin$	$\in$ ou $\notin$	$\in$ ou $\notin$	
C_1	$\in$ ou $\notin$	$\boxed{\in \text{ ou } \notin}$	$\in$ ou $\notin$	$\in$ ou $\notin$	
C_2	$\in$ ou $\notin$	$\in$ ou $\notin$	$\boxed{\in \text{ ou } \notin}$	$\in$ ou $\notin$	
C_3	$\in$ ou $\notin$	$\in$ ou $\notin$	$\in$ ou $\notin$	$\boxed{\in \text{ ou } \notin}$	
$\vdots$					

Outro conjunto não contável

O conjunto das funções $f : \mathbf{N} \to \mathbf{N}$ não é contável:

	0	1	2	3	$\cdots$
f_0	$\boxed{f_0(0)}$	$f_0(1)$	$f_0(2)$	$f_0(3)$	
f_1	$f_1(0)$	$\boxed{f_1(1)}$	$f_1(2)$	$f_1(3)$	
f_2	$f_2(0)$	$f_2(1)$	$\boxed{f_2(2)}$	$f_2(3)$	
f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$\boxed{f_3(3)}$	
$\vdots$					

O que é definição recursiva

Definição recursiva do conjunto A

(a) **Base**: especificação de $B \subset A$.

(b) **Passo recursivo**: como obter elementos de A a partir de elementos de A.

(c) **Fechamento**: só pertencem a A os referidos em (a) e (b).

Definição recursiva dos naturais

O conjunto $\mathbf{N}$ pode ser definido assim:

a) $0 \in \mathbf{N}$;

b) se $n \in \mathbf{N}$, então $s(n) \in \mathbf{N}$;

c) só pertence a $\mathbf{N}$ o número que pode ser obtido de acordo com (a) e (b).

Definição recursiva de fatorial

A função fatorial, $fat : \mathbf{N} \to \mathbf{N}$ é definida recursivamente por:

a) $fat(0) = 1$;

b) $fat(n) = n \times fat(n-1)$, para $n \geq 1$.

Definição recursiva de soma

Definição recursiva da função $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$:

a) $n + 0 = n$, para todo $n \in \mathbf{N}$;

b) $m + s(n) = s(m + n)$, para todo $m, n \in \mathbf{N}$.

Definição recursiva da linguagem proposicional

Definição recursiva da linguagem LP da lógica proposicinal:

a) cada variável proposicional pertence a LP;

b) se α e β pertencem a LP, então também pertencem a LP:

- $\neg\alpha$;
- $(\alpha \land \beta)$;
- $(\alpha \lor \beta)$;
- $(\alpha \to \beta)$;
- $(\alpha \leftrightarrow \beta)$.

(Cláusula de fechamento implícita.)

Indução fraca

Baseada na validade de $[P(0) \land \forall n(P(n) \to P(n+1))] \to \forall n P(n)$:

Princípio de indução fraca

Se

1. $P(0)$, e
2. $\forall n(P(n) \to P(n+1))$,

então $\forall n P(n)$.

Estrutura de demonstração por indução fraca

1. Provar $P(0)$.
2. Seja $n \geq 0$ arbitrário.
3. Suponha $(P(n)$ (**hipótese de indução**).
4. Provar $P(n+1)$.
5. Concluir $\forall n P(n)$.

Uso de indução fraca

Exemplos:

- $\sum_{k=0}^{n} k = n(n+1)/2$.
- $n! > 2^n$ para todo $n \geq 4$.

Indução forte:

Baseada na validade de $\forall n(\forall k < nP(k) \rightarrow P(n)) \rightarrow \forall nP(n)$:

Princípio de indução forte

Se

- $\forall n\,(\forall k < nP(k) \rightarrow P(n))$

então $\forall nP(n)$.

Estrutura de demonstração por indução forte

1. Seja $n \geq 0$ arbitrário.
2. Suponha $\forall k < n\,P(k)$ (**hipótese de indução**).
3. Provar $P(n+1)$.
4. Concluir $\forall nP(n)$.

Uso de indução forte

Função de Fibonacci:

a) $F_0 = 0$; $F_1 = 1$;

b) $F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$.

Exemplos:

- $F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$.
- $\mathrm{na}(\alpha) = \mathrm{na}(\beta)$ para toda $\alpha \in \mathrm{LP}$.

O que é grafo

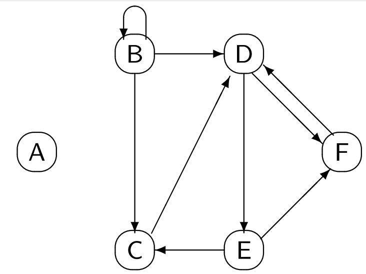
Grafo

Um grafo é um par (V, A), sendo
V um conjunto de **vértices** e
A um conjunto de **arestas**.

Grafo **dirigido**: as arestas são pares ordenados.

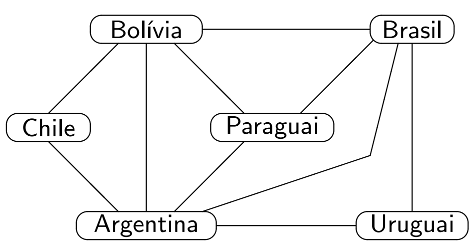
Grafo **não dirigido**: as arestas são pares não ordenados.

Exemplo de grafo dirigido



- Vértices: $\{A, B, C, D, E, F\}$.
- Arestas: $\{(B, B), (B, C), (B, D), (D, E), \ldots\}$.

Exemplo de grafo não dirigido



- Vértices: $\{\text{Brasil}, \text{Bolívia}, \ldots\}$.
- Arestas: $\{\{\text{Bolívia}, \text{Chile}\}, \{\text{Bolívia}, \text{Brasil}\}, \ldots\}$.

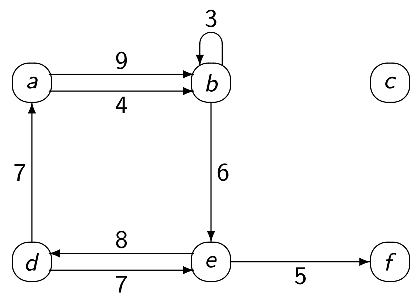
Grafos rotulados

Grafos podem ter **rótulos** associados a suas arestas e/ou vértices.

Grafo dirigido rotulado

Um grafo dirigido rotulado é uma tripla (V, A, R),
sendo V um conjunto de **vértices**,
A um conjunto de **arestas rotuladas**, e
R um conjunto de **rótulos**.

Um exemplo de grafo dirigido rotulado



- Vértices: $\{a, b, c, d, e, f\}$.
- Arestas: $\{(a, 4, b), (a, 9, b), (b, 3, b), \ldots\}$.

Alguns conceitos importantes

Grau de um vértice

Número de arestas incidentes ao vértice.

Caminho de comprimento n de a para b

Sequência de vértices e arestas $v_0 x_1 v_1 x_2 v_2 \ldots v_{n-1} x_n v_n$ tal que:

- $v_0 = a$;
- $v_n = b$; e
- $x_i = (v_{i-1}, v_i)$.

Caminhos

- Caminho **nulo**: caminho de comprimento zero.
- Caminho **fechado**: aquele em que $v_0 = v_n$.
- **Ciclo**: caminho fechado sem vértices e arestas repetidos, exceto v_0 e v_n.
- **Laço**: ciclo de comprimento 1.
- **Caminho simples**: caminho sem vértices repetidos.
- Grafo **acíclico**: grafo sem ciclos.
- Grafo **conexo**: aquele em que existe caminho de qualquer vértice a qualquer outro.

Árvore

Uma árvore é um grafo acíclico conexo.

Árvore com raiz

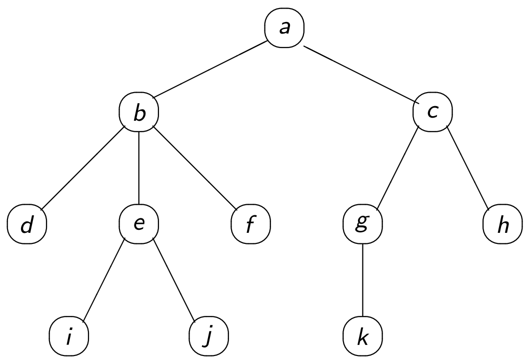
Uma árvore com raiz é uma tripla (V, A, r) tal que

a) $(\{v\}, \emptyset, v)$ é árvore;

b) se (V, A, r) é uma árvore, $v \in V$ e $v' \notin V$, então $V \cup \{v'\}, A \cup \{\{v, v'\}\}, r)$ é árvore;

c) nada mais é árvore.

Exemplo de árvore com raiz



Terminologia associada a árvores

- Filhos, pais, irmãos, descendente, ancestral.
- Vértice **interno**, **folha**.
- **Nível** de um vértice; **altura** da árvore.
- Árvore **dirigida**; **ordenada**.
- **Fronteira** de uma árvore.

Conceitos iniciais

Alfabeto

Conjunto finito não vazio (de *símbolos*).

Exemplos:

- $\{1\}$.
- $\{0, 1\}$.
- $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$.
- Conjunto dos caracteres do teclado.

Conceitos iniciais

Palavra (string) em um alfabeto Σ

Sequência finita de símbolos de Σ.

Exemplos de palavras em $\{0, 1\}$:

- λ (a palavra vazia), 0, 1, 00, 01, 10, 11, 000 etc.

Comprimento de uma palavra w

$|w| =$ número de símbolos de w.

Notação

a^n abrevia n as em sequência.

Exemplos:

- $1^0 = \lambda$.
- $0^4 = 0000$.
- $1^3 01^2 = 111011$.
- $1^{1000} =$ ops...

Σ^* é o conjunto de todas as palavras sobre Σ.

Exemplos:

- $\{1\}^* = \{\lambda, 1, 11, 111, 1^4, 1^5, \ldots\}$.
- $\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, \ldots\}$.

Linguagem

Linguagem de alfabeto Σ

Uma linguagem sobre Σ é um subconjunto de Σ^*.

Exemplos de linguagens sobre $\{0,1\}$:

- $\emptyset$.
- $\{\lambda\}$.
- $\{\lambda, 0\}$.
- $\{w \in \Sigma^* \mid 1 \leq |w| \leq 5\}$.
- $\{0^n \mid n$ é um número primo$\}$.
- $\{0^n 1^n \mid n \in \mathbf{N}\}$.
- $\{0,1\}^*$.

Operações sobre conjuntos se aplicam a linguagens

Sejam as linguagens L_1 sobre Σ_1 e L_2 sobre Σ_2. Então:

- $L_1 \cup L_2$ é uma linguagem sobre $\Sigma_1 \cup \Sigma_2$;
- $L_1 \cap L_2$ é uma linguagem sobre $\Sigma_1 \cap \Sigma_2$;
- $L_1 - L_2$ é uma linguagem sobre Σ_1;
- $\overline{L_1} = \Sigma_1^* - L_1$ é uma linguagem sobre Σ_1;
- $\mathcal{P}(L_1)$ é um conjunto de linguagens sobre Σ_1;
- $\mathcal{P}(\Sigma_1^*)$ é o conjunto de todas as linguagens sobre Σ_1.

Concatenação

Concatenação de palavras

A concatenação de $x = a_1 a_2 \ldots a_m$ e $y = b_1 b_2 \ldots b_n$ é $xy = a_1 a_2 \ldots a_m b_1 b_2 \ldots b_n$.

Exemplos:

- se $x = 001$ e $y = 10$, então $xy = 00110$
- $\lambda w = w \lambda = w$ para qualquer palavra w.
- $x(yz) = (xy)z$ para quaisquer palavras x, y e z. Assim, pode-se escrever sem parênteses: xyz.

Uma operação e uma propriedade de palavras

Reverso

O reverso de $w = a_1a_2 \ldots a_n$ é $w^R = a_na_{n-1} \ldots a_1$.

Exemplos: $\lambda^R = \lambda$; $\mathtt{a}^R = \mathtt{a}$; $(\mathtt{abcaabb})^R = \mathtt{bbaacba}$.

Palíndromo

Uma palavra w tal que $w = w^R$.

Exemplos: λ, a, bb, ccc, aba, baab, abcba.

Prefixos, sufixos e subpalavras de uma palavra

Prefixo, sufixo, subpalavra

Prefixo de w: palavra x tal que $w = xy$.

Sufixo de w: palavra y tal que $w = xy$.

Subpalavra de w: palavra z tal que $w = xzy$.

Exemplos:

- Prefixos de abc: λ, a, ab e abc.
- Sufixos de abc: λ, c, bc e abc.
- Subpalavras de abc: λ, a, b, c, ab, bc e abc.

Concatenação de linguagens

Concatenação de L_1 e L_2

$$L_1L_2 = \{xy \mid x \in L_1 \text{ e } y \in L_2\}.$$

Exemplos: Sejam $L_1 = \{w \in \{0,1\}^* \mid |w| = 5\}$ e
$L_2 = \{0y \mid y \in \{0,1\}^*\}$

- $\emptyset L_1 = \emptyset$; $\{\lambda\}L_1 = L_1$;
- $L_1L_1 = \{w \in \{0,1\}^* \mid |w| = 10\}$;
- $L_1L_2 = \{w \in \{0,1\}^* \mid |w| \geq 6 \text{ e o sexto símbolo de } w \text{ é } 0\}$;
- $L_2L_1 = \{w \in \{0,1\}^* \mid |w| \geq 6 \text{ e } w \text{ começa com } 0\}$;
- $L_2L_2 = \{0y \mid y \in \{0,1\}^* \text{ e } y \text{ contém no mínimo um } 0\}$.

Fecho de Kleene de uma linguagem

L^n designa $LL \ldots L$ (n vezes). $L^0 = \{\lambda\}$ (por que?).

Fecho de Kleene de L

L^*, pode ser definida recursivamente assim:

a) $\lambda \in L^*$;

b) se $x \in L^*$ e $y \in L$, então $xy \in L^*$.

Pode-se mostrar que:

$$L^* = \bigcup_{n \in \mathbf{N}} L^n = L^0 \cup L^1 \cup L^2 \cup \cdots = \{\lambda\} \cup L \cup LL \cup \cdots.$$

Fecho positivo de Kleene de uma linguagem

Fecho positivo de Kleene de L

$L^+ = LL^*$

Pode-se mostrar que:

$$L^+ = \bigcup_{n \geq 1} L^n = L^1 \cup L^2 \cup \cdots = L \cup LL \cup \cdots.$$

Segue diretamente das definições que $L^* = L^+ \cup \{\lambda\}$.

Exemplificando fechos de Kleene

- $\emptyset^* = \{\lambda\}$, e $\emptyset^+ = \emptyset$;
- $\{\lambda\}^* = \{\lambda\}^+ = \{\lambda\}$;
- $\{0\}^* = \{0^n \,|\, n \in \mathbf{N}\}$ e $\{0\}^+ = \{0^n \,|\, n \geq 1\}$;
- $\{00\}^* = \{w \in \{0\}^* \,|\, |w|$ é par$\}$ e $\{00\}^+ = \{w \in \{0\}^* \,|\, |w|$ é par e $|w| \geq 2\}$.
- $\{01, 1\}^* = \{w \in \{0,1\}^* \,|$ todo 0 em w é seguido de $1\}$.
- $\{\lambda, 00, 11\}^* = \{\lambda, 00, 11\}^+ = \{\lambda\} \cup \{00, 11\}^+$.

Descrevendo linguagens por meio das operações vistas

- o conjunto das palavras que começam com 0: $\{0\}\{0,1\}^*$;
- o conjunto das palavras que contêm 00 ou 11: $\{0,1\}^*\{00,11\}\{0,1\}^*$;
- o conjunto das palavras que terminam com 0 seguido de um número ímpar de 1s consecutivos: $\{0,1\}^*\{01\}\{11\}^*$;
- o conjunto das palavras de tamanho par que começam com 0 ou terminam com 0: $(\{0,1\}\{0,1\})^* \cap [\{0\}\{0,1\}^* \cup \{0,1\}^*\{0\}]$;
- o conjunto anterior: $[\{0\}\{0,1\}(\{0,1\}\{0,1\})^*] \cup [\{0,1\}(\{0,1\}\{0,1\})^*\{0\}]$;

Exemplos de linguagens não tão "fáceis"

- o conjunto das palavras com um prefixo de um ou mais 0s seguido (imediatamente) de um sufixo de 1s de mesmo tamanho: $\{0^n1^n \mid n \geq 1\}$;
- o conjunto das palavras formadas por concatenações de palavras da forma 0^n1^n para $n \geq 1$: $\cup_{k \geq 1}\{0^n1^n \mid n \geq 1\}^k$.
- o conjunto das palavras de tamanho par com as duas metades idênticas: $\{xx \,|\, x \in \{0,1\}^*\}$.

Definição recursiva de linguagens

- Σ^* é enumerável.
- Logo, pode-se fazer uma definição recursiva de uma linguagem.
  Exemplo:
  a) $\lambda \in L$;
  b) se $x \in L$ então $0x1 \in L$.
- **Gramática**: formalismo, que permite o uso de recursão, especialmente projetado para a definição de linguagens.

Conceitos envolvidos em gramáticas

- Alfabeto de **terminais**: alfabeto da linguagem definida.
  Exemplo: $\Sigma = \{\mathtt{0}, \mathtt{1}\}$.
- Alfabeto de **variáveis** (não terminais): de símbolos auxiliares.
  Exemplo: $\Gamma = \{\mathtt{A}, \mathtt{B}\}$.
- **Regra**: par ordenado (u, v), tradicionalmente escrito na forma $u \to v$. Exemplo: $0AB \to 10A$.

Um exemplo de derivação

Derivação (geração) de $110A10A$ a partir de $0ABB0AB$:

$$\begin{aligned} 0ABB0AB &\Rightarrow 10AB0AB && \text{(aplicando-se a regra } 0AB \to 10A) \\ &\Rightarrow 110A0AB && \text{(aplicando-se a regra } 0AB \to 10A) \\ &\Rightarrow 110A10A && \text{(aplicando-se a regra } 0AB \to 10A) \end{aligned}$$

Definição informal de gramática

- Uma gramática é constituída de uma **variável de partida** e um **conjunto de regras**.
- Toda derivação deve iniciar pela variável de partida.
- **Forma sentencial**: palavra constituída de terminais e/ou variáveis.
- **Sentença**: forma sentencial constituída de terminais apenas.
- **Linguagem gerada**: sentenças que podem ser derivadas.

Notação: $L(G)$ é a linguagem gerada pela gramática G.

Dois exemplos de gramática

A gramática de variável P e as duas regras a seguir gera $\{0\}^*$:

1. $P \rightarrow 0P$
2. $P \rightarrow \lambda$

A gramática de variável P e as duas regras a seguir gera $\{0^n 1^n \mid n \geq 0\}$:

1. $P \rightarrow 0P1$
2. $P \rightarrow \lambda$

Um outro exemplo de gramática

Seja a gramática G constituída pela variável de partida P e pelas regras:

1. $P \rightarrow \mathtt{a}A\mathtt{bc}$
2. $A \rightarrow \mathtt{a}A\mathtt{b}C$
3. $A \rightarrow \lambda$
4. $C\mathtt{b} \rightarrow \mathtt{b}C$
5. $C\mathtt{c} \rightarrow \mathtt{cc}$

Um exemplo de derivação

$$
\begin{aligned}
P &\Rightarrow \mathtt{a}A\mathtt{bc} && \text{(regra 1)}\\
&\Rightarrow \mathtt{abc} && \text{(regra 3)}
\end{aligned}
$$

Isso mostra que $\mathtt{abc} \in L(G)$.

Outra derivação

$$
\begin{aligned}
P &\Rightarrow \mathtt{a}A\mathtt{bc} && \text{(regra 1)}\\
&\Rightarrow \mathtt{aa}A\mathtt{b}C\mathtt{bc} && \text{(regra 2)}\\
&\Rightarrow \mathtt{aaa}A\mathtt{b}C\mathtt{b}C\mathtt{bc} && \text{(regra 2)}\\
&\Rightarrow \mathtt{aaab}C\mathtt{b}C\mathtt{bc} && \text{(regra 3)}\\
&\Rightarrow \mathtt{aaabb}CC\mathtt{bc} && \text{(regra 4)}\\
&\Rightarrow \mathtt{aaabb}C\mathtt{b}C\mathtt{c} && \text{(regra 4)}\\
&\Rightarrow \mathtt{aaabb}C\mathtt{bcc} && \text{(regra 5)}\\
&\Rightarrow \mathtt{aaabbb}C\mathtt{cc} && \text{(regra 4)}\\
&\Rightarrow \mathtt{aaabbbccc} && \text{(regra 5)}
\end{aligned}
$$

Logo, $\mathtt{a}^3\mathtt{b}^3\mathtt{c}^3 \in L(G)$. O que é $L(G)$?

Definição de gramática

Gramática

Uma gramática é uma quádrupla (V, Σ, R, P), em que:

a) V é um conjunto finito de elementos denominados *variáveis*;

b) Σ é um alfabeto; $V \cap \Sigma = \emptyset$;

c) $R \subseteq (V \cup \Sigma)^{+} \times (V \cup \Sigma)^{*}$ é um conjunto finito de pares ordenados chamados *regras*; e

d) $P \in V$ é uma variável conhecida como *variável de partida*.

Derivação em n passos

$\overset{n}{\Rightarrow}$

A relação $\overset{n}{\Rightarrow}$ é definida recursivamente assim para uma gramática G:

a) $x \overset{0}{\Rightarrow} x$ para toda forma sentencial x de G;

b) se $w \overset{n}{\Rightarrow} xuy$ e $u \rightarrow v$ é regra de G, então $w \overset{n+1}{\Rightarrow} xvy$.

Derivação em vários passos

$\overset{*}{\Rightarrow}$

$x \overset{*}{\Rightarrow} y$, se existe $n \geq 0$ tal que $x \overset{n}{\Rightarrow} y$.

$\overset{+}{\Rightarrow}$

$x \overset{+}{\Rightarrow} y$, se existe $n \geq 1$ tal que $x \overset{n}{\Rightarrow} y$.

A linguagem gerada por uma gramática

$L(G)$

Seja $G = (V, \Sigma, R, P)$.

$$L(G) = \{w \in \Sigma^* \mid P \overset{*}{\Rightarrow} w\}.$$

Esquema de derivação/Exemplo

$$
\begin{array}{lll}
P & \Rightarrow \mathtt{a}A\mathtt{bc} & \text{(regra 1)} \\
 & \overset{k}{\Rightarrow} \mathtt{aa}^k A(\mathtt{b}C)^k\mathtt{bc} & \text{(regra 2, } k \text{ vezes; } k \geq 0) \\
 & \Rightarrow \mathtt{aa}^k(\mathtt{b}C)^k\mathtt{bc} & \text{(regra 3)} \\
 & \Rightarrow \mathtt{a}^{k+1}(\mathtt{b}C)^{k-1}\mathtt{b}^2C\mathtt{c} & \text{(regra 4, 1 vez)} \\
 & \overset{2}{\Rightarrow} \mathtt{a}^{k+1}(\mathtt{b}C)^{k-2}\mathtt{b}^3C^2\mathtt{c} & \text{(regra 4, 2 vezes)} \\
 & \vdots & \\
 & \overset{k}{\Rightarrow} \mathtt{a}^{k+1}\mathtt{b}^{k+1}C^k\mathtt{c} & \text{(regra 4, } k \text{ vezes)} \\
 & \overset{k}{\Rightarrow} \mathtt{a}^{k+1}\mathtt{b}^{k+1}\mathtt{c}^{k+1} & \text{(regra 5, } k \text{ vezes)}
\end{array}
$$

Logo, conclui-se que $\{\mathtt{a}^n\mathtt{b}^n\mathtt{c}^n \mid n \geq 1\} \subseteq L(G)$.

Equivalência de gramáticas

Gramáticas equivalentes

Duas gramáticas G e G' são ditas equivalentes quando $L(G) = L(G')$.

Notação simplificada

Duas regras com o mesmo lado esquerdo:

$u \rightarrow v$ e $u \rightarrow v'$

podem ser escritas assim:

$u \rightarrow v \mid v'$

As regras 2 e 3 do exemplo seriam podem ser expressas assim:

$A \rightarrow \mathtt{a}A\mathtt{b}C \mid \lambda$

Um outro exemplo de gramática

$G = (V, \Sigma, R, E)$, em que:

- $V = \{E, T, N, D\}$;
- $\Sigma = \{+, -, (,), 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$;
- R contém as regras:

$$
\begin{array}{l}
E \rightarrow E + T \mid E - T \mid T \\
T \rightarrow (E) \mid N \\
N \rightarrow DN \mid D \\
D \rightarrow 0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9
\end{array}
$$

Exemplo de derivação

Gerando sequência de somas e/ou subtrações de Ts:

$$\begin{aligned} E &\Rightarrow E+T && (\text{regra } E \to E+T) \\ &\Rightarrow E-T+T && (\text{regra } E \to E-T) \\ &\Rightarrow E-T-T+T && (\text{regra } E \to E-T) \\ &\Rightarrow T-T-T+T && (\text{regra } E \to T) \end{aligned}$$

$\Longrightarrow$ recursão à esquerda.

Exemplo de derivação

Gerando sequência de 4 dígitos:

$$\begin{aligned} N &\Rightarrow DN && (\text{regra } N \to DN) \\ &\Rightarrow DDN && (\text{regra } N \to DN) \\ &\Rightarrow DDDN && (\text{regra } N \to DN) \\ &\Rightarrow DDDD && (\text{regra } N \to D) \end{aligned}$$

$\Longrightarrow$ recursão à direita.

Exemplo de derivação

$$\begin{aligned} E &\Rightarrow E+T && (\text{regra } E \to E+T) \\ &\Rightarrow T+T && (\text{regra } E \to T) \\ &\Rightarrow (E)+T && (\text{regra } T \to (E)) \end{aligned}$$

$\Longrightarrow$ a variável E aparece (recursivamente) na forma sentencial entre "(" e ")".

O que é problema de decisão

Problema de decisão

Um problema de decisão é uma questão que faz referência a um conjunto finito de parâmetros e que, para valores específicos dos parâmetros, tem como resposta *sim* ou *não*.

Exemplos de problemas de decisão

a) determinar se o número 123654789017 é um número primo;

b) determinar se um número natural n é um número primo;

c) determinar se existe um ciclo em um grafo G;

d) determinar se uma palavra w é gerada por uma gramática G.

Instâncias de um problema de decisão

Instância de um PD: cada questão obtida dando aos parâmetros valores específicos.

Exemplo: o PD "determinar se um número natural n é um número primo" tem um conjunto infinito de instâncias:

- determinar se 0 é um número primo;
- determinar se 1 é um número primo;
- determinar se 2 é um número primo;
- e assim por diante.

O PD "determinar se 123654789017 é um número primo" tem uma única instância.

Solução para um problema de decisão

Solução

Uma solução para um PD, denominada **procedimento de decisão**, é um *algoritmo* que, para qualquer instância do PD, retorna a resposta correta.

Problema decidível

Problema decidível

Um PD que tem solução é dito ser *decidível*, e um PD que não tem solução, *indecidível*.

$\Longrightarrow$ Todo PD com conjunto finito de instâncias é decidível!

Restrição de um problema de decisão

Restrição de um PD

Um PD obtido de outro, P, restringindo-se o conjunto de valores possíveis de um ou mais parâmetros de P.

Exemplos:

- "determinar se 123654789017 é um número primo" é uma restrição de "determinar se um número natural n é um número primo".
- "determinar se uma palavra w é gerada por uma gramática G_0 sensível ao contexto, é uma restrição de "determinar se uma palavra w é gerada por uma gramática G".