Linguagens Formais e Autômatos

Humberto Longo

Instituto de Informática
Universidade Federal de Goiás

Bacharelado em Ciência da Computação, 2022/2

Notação

- Conjunto: coleção não ordenada de elementos.
- $S = \{x \mid P(x)\}$ (P é um predicado unário).
- $S = \{x \mid P(x)\} \equiv (\forall\, x)[(x \in S \Rightarrow P(x)) \wedge (P(x) \Rightarrow x \in S)]$.
- Conjuntos padrões:
  - $\mathbb{N}$: inteiros não negativos ($0 \in \mathbb{N}$).
  - $\mathbb{Z}$: inteiros.
  - $\mathbb{Q}$: racionais.
  - $\mathbb{R}$: reais.
  - $\mathbb{C}$: complexos.
  - $\varnothing$: conjunto vazio.

Notação

- $A \subsetneq B \equiv A \subset B \equiv A \subseteq B$ e $A \neq B$: subconjunto próprio.
- $A = B \Rightarrow A \subseteq B$ e $B \subseteq A$.
- Para qualquer conjunto $S \neq \varnothing$:
  - $S \subseteq S$: subconjunto impróprio.
  - $\varnothing \subset S$: $\varnothing$ é subconjunto próprio de qualquer conjunto S.
- $P(S)$: conjunto das partes de S.
  - conjunto potência de S.
  - todos os subconjuntos de S.
  - $|P(S)| = 2^{|S|}$. (Exercício: Provar esta igualdade.)

Operações em conjuntos

- $\mathbb{U}$: conjunto universo.
- $A - B = \{x \in \mathbb{U} \mid x \in A$ e $x \notin B\}$.
- $A \cap B = \{x \in \mathbb{U} \mid x \in A$ e $x \in B\}$.
- $A \cup B = \{x \in \mathbb{U} \mid x \in A$ ou $x \in B\}$.
- $\overline{A}$: complemento do conjunto A.
  - $\overline{A} = \{x \mid x \in \mathbb{U}$ e $x \notin A\}$.
  - $\overline{A} = A' = A^{\mathsf{c}} = \complement_{\mathbb{U}}^{A}$.
  - $\overline{A} \cap A = \varnothing$ e $\overline{A} \cup A = \mathbb{U}$.
  - $\complement_{B}^{A}$ quando $A \subseteq B$.
  - $\complement_{A}^{B}$ quando $B \subseteq A$.

Produto cartesiano

- $A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$
- $\bigtimes_{i=1}^{n} A_i = A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}$
- $A_i = A, i = 1, \ldots, n \Rightarrow \bigtimes_{i=1}^{n} A_i = A^n$

Propriedades

- $A \subseteq (A \cup B)$ e $B \subseteq (A \cup B)$.
  - $(A \cap B) \subseteq A$ e $(A \cap B) \subseteq B$.
- $A \subseteq D$ e $B \subseteq D \Rightarrow (A \cup B) \subseteq D$.
  - $D \subseteq A$ e $D \subseteq B \Rightarrow D \subseteq (A \cap B)$.
- $|A \cup B| \leqslant |A| + |B|$.
- $|A \cap B| \leqslant \min\{|A|, |B|\}$.
- $|A - B| \leqslant |A|$.
- $|A \times B| \leqslant |A|.|B|$.

Princípio da inclusão e da exclusão

- $|A \cup B| = |A| + |B| - |A \cap B|$.
- $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.
- $$|A_1 \cup \cdots \cup A_n| = \begin{cases} \sum_{i=1}^{n} |A_i| & - \\ \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| & + \\ \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| & - \\ \vdots & + \\ (-1)^{n+1} |A_1 \cap \cdots \cap A_n|. \end{cases}$$

Leis da álgebra de conjuntos

- Comutativas:
  - $A \cup B = B \cup A$.
  - $A \cap B = B \cap A$.
- Associativas:
  - $(A \cup B) \cup C = A \cup (B \cup C)$.
  - $(A \cap B) \cap C = A \cup (B \cap C)$.
- Distributivas:
  - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
  - $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
- Identidades:
  - $(A \cup \varnothing) = A$.
  - $(A \cup \mathbb{U}) = \mathbb{U}$.
  - $(A \cap \varnothing) = \varnothing$.
  - $(A \cap \mathbb{U}) = A$.

Leis da álgebra de conjuntos

- Idempotentes:
  - $(A \cup A) = A$.
  - $(A \cap A) = A$.
- Complementação:
  - $(A \cup A^c) = \mathbb{U}$.
  - $(A \cap A^c) = \varnothing$.
  - $\mathbb{U}^c = \varnothing$.
  - $\varnothing^c = \mathbb{U}$.
  - $(A^c)^c = A$.
- DeMorgan:
  - $(A \cup B)^c = A^c \cap B^c$.
  - $(A \cap B)^c = A^c \cup B^c$.
  - $A - (B \cup C) = (A - B) \cap (A - C)$.
  - $A - (B \cap C) = (A - B) \cup (A - C)$.

Partição de um conjunto

- $\Pi = \{A_i \subset A \mid i \in I\}$.
  - I : conjunto de índices (não necessariamente finito).
  - A : conjunto qualquer.
- Π é uma partição de A se:
  - $A_i \cap A_j = \varnothing$, $\forall\, i \neq j$, $i, j \in I$.
  - $\bigcup_{i \in I} A_i = A$.

Relação binária

- $R \subseteq A \times A$:
  - $a\,R\,b \Leftrightarrow (a, b) \in R$.
- $R_1 = \{(x, y) \mid x = y + 1\} \subseteq \mathbb{N} \times \mathbb{N}$.
- $R_2 = \{(x, y) \mid x + y$ é impar$\} \subseteq \mathbb{N} \times \mathbb{N}$.
- $R_3 = \{(x, y) \mid x \cdot y$ é par$\} \subseteq \mathbb{N} \times \mathbb{N}$.

Tipos de relação

- A, B : conjuntos finitos.
- $R = \{(a, b) \mid a \in A$ e $b \in B\}$:
  - um-para-um (injetiva, biunívoca);
  - um-para-vários;
  - vários-para-um (unívoca); e
  - vários-para-vários.
- Relação inversa:
  - $R = \{(a, b) \mid a \in A$ e $b \in B\}$.
  - $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$.

Operações com relações

- R_1, R_2 : relações definidas no conjunto finito $S \neq \emptyset$.
- $x(R_1 \cup R_2)y \Leftrightarrow xR_1y$ ou xR_2y.
- $x(R_1 \cap R_2)y \Leftrightarrow xR_1y$ e xR_2y.
- $x(R_1^c)y \Leftrightarrow x\not R_1 y \ ((x,y) \notin R_1)$.

Propriedades

- R : relação definida no conjunto finito $S \neq \emptyset$.

Reflexiva : $xRx, \ \forall x \in S$.

Irreflexiva : $x\not Rx, \ \forall x \in S \ \ ((x,x) \notin R)$.

Simétrica : $xRy \Rightarrow yRx, \ \forall x, y \in S$.

Antissimétrica : xRy e $yRx \Rightarrow x = y, \ \forall x, y \in S$.

Antissimétrica : $x \neq y \Rightarrow x\not Ry$ ou $y\not Rx$.

Transitiva : xRy e $yRz \Rightarrow xRz, \ \forall x, y, z \in S$.

Fecho de uma relação

- R, R^* : relações definidas no conjunto finito $S \neq \emptyset$.
- R^* é o fecho de R em relação à propriedade P se:
  - R^* tem a propriedade P;
  - $R \subseteq R^*$;
  - R^* é o menor conjunto que satisfaz os itens anteriores;
  - R^* é subconjunto de qualquer outra relação em S que inclui R e tem a propriedade P.

Fecho de uma relação

Exemplo 1.1

- $S = \{1, 2, 3\}$.
- $R = \{(1,1), (1,2), (1,3), (3,1), (2,3)\}$.
  - Fecho reflexivo: $\{(1,1), (1,2), (1,3), (3,1), (2,3), (2,2), (3,3)\}$.
  - Fecho simétrico: $\{(1,1), (1,2), (1,3), (3,1), (2,3), (2,1), (3,2)\}$.
  - Fecho transitivo: $\{(1,1), (1,2), (1,3), (3,1), (2,3), (3,2), (3,3), (2,1), (2,2)\}$.

Ordem parcial

- R : relação definida no conjunto finito $S \neq \emptyset$.
- R é de ordem parcial se é reflexiva, antissimétrica e transitiva:
  - $\forall\, x \in S \Rightarrow xRx$.
  - $\forall\, x, y \in S,\ xRy$ e $yRx \Rightarrow x = y$.
  - $\forall\, x, y, z \in S,\ xRy$ e $yRz \Rightarrow xRz$.
- $x \preceq y(R) \equiv (x, y) \in R$:
  - x precede y na relação R.

Ordem total

- R : relação definida no conjunto finito $S \neq \emptyset$.
- R é de ordem total se:
  - R é de ordem parcial.
  - $\forall\, x, y \in S \Rightarrow x \preceq y(R)$ ou $y \preceq x(R)$.

Relação de equivalência

- R : relação definida no conjunto finito $S \neq \emptyset$.
- R é relação de equivalência se e somente se é reflexiva, simétrica e transitiva:
  - $\forall\, x \in S \Rightarrow xRx$.
  - $\forall\, x, y \in S,\ xRy \Rightarrow yRx$.
  - $\forall\, x, y, z \in S,\ xRy$ e $yRz \Rightarrow xRz$.
- $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x - y = 3{\cdot}k$ para algum $k \in \mathbb{Z}\}$.

Classe de equivalência

- R : relação definida no conjunto finito $S \neq \emptyset$.
- $\overline{a} = \{x \in S \mid xRa$ e $a \in S\}$: classe de equivalência módulo R determinada por a.
- S/R : conjunto das classes de equivalência módulo R.

Teorema 1.2

- *Se R é relação de equivalência sobre o conjunto S, então S/R é partição de S.*

Teorema 1.3

- *Se Π é uma partição do conjunto S, então existe uma relação R de equivalência sobre S, de modo que $S/R = \Pi$.*

Relação n-ária

- $S_1, S_2, \cdots, S_n$ – conjuntos.
- Relação n-ária em $S_1, S_2, \cdots, S_n$:
  - Subconjunto de $S_1 \times S_2 \times \cdots \times S_n$.
- Relação unária R em um conjunto S :
  - $R \subseteq S$.
  - $x \in S$ satisfaz R se e somente se $x \in R$.
- Relação n-ária R em um conjunto S :
  - $R \subseteq S^n$.
  - Conjunto de n-uplas ordenadas de elementos de S .

Funções

Definição

- $f : A\,R\,B \subset A \times B$: função de um conjunto A no conjunto B.
  - Cada elemento de A aparece exatamente uma vez como primeiro componente de um par ordenado de f.
  - Método para associar cada $a \in A$ a um único $b \in B$. Logo, se $(a, b), (a, c) \in f \Rightarrow b = c$.

Funções

Notação

- $f : A\,R\,B$ $(f : A \to B)$:
  - A é o domínio $(D(f))$ e B o contradomínio de f.
  - $(a, b) \in f \Rightarrow f(a) = b$.
  - b é a imagem de a por f.
  - a é a pré-imagem de b por f.
- Uma relação R de A em B é uma função $f : A \to B$ se:
  - $D(f) = A$;
  - Dado $a \in D(f)$, é único o elemento $b \in B$ tal que $(a, b) \in f$.

Funções

Propriedades

- Uma função $f : A \to B$ pode ser:
  - Injetora: $\forall\, b \in B$, $\exists$ no máximo um $a \in A$ tal que $f(a) = b$.
  - Sobrejetora: $\forall\, b \in B$, $\exists$ pelo menos um $a \in A$ tal que $f(a) = b$.
  - Bijetora: $\forall\, b \in B$, $\exists$ exatamente um $a \in A$ tal que $f(a) = b$.

Funções

Função identidade

- $f : A \to A$ é identidade (i_A) se $f(a) = a$, $\forall\, a \in A$.

Função composta

- $f : A \to B$.
- $g : B \to C$.
- $g \circ f : A \to C$.
- $(g \circ f)(a) = g(f(a))$.

Teorema 1.4

- *Se $f : A \to B$ e $g : B \to C$ são bijeções, então $(g \circ f)$ é uma bijeção.*

Funções

Função inversa

- Seja $f : A \to B$. Se existir $g : B \to A$ tal que $(g \circ f) = i_A$ e $(f \circ g) = i_B$, g é chamada de inversa de f (denotada por f^{-1}).

Teorema 1.5

- *Seja $f : A \to B$. f é uma bijeção se e somente se f^{-1} existe.*

Conjuntos equinumerosos

- A, B : conjuntos quaisquer.
- A e B são equinumerosos se existir uma bijeção $f : A \to B$.
  - Se existe $f : A \to B$, então existe $f^{-1} : A \to B$.
  - Equinumerosidade é uma relação de equivalência.

Conjuntos finitos e infinitos

- Um conjunto é:
  - Finito se ele é equinumeroso com $\{1, 2, \ldots, n\}$, para algum $n \in \mathbb{N}$.
  - Infinito se ele não é finito!!!
  - Contavelmente infinito se é equinumeroso com $\mathbb{N}$.

Método da diagonalização

- Georg Cantor, 1873.
- Problema da medição do tamanho de conjuntos infinitos.
  - Dados dois conjuntos infinitos, os dois são de mesmo tamanho ou um deles é maior que o outro?
  - Ex: $P = \{n = 2{\cdot}k \mid k \in \mathbb{Z}^+\}$ e $S = \{s \mid s \in \{0,1\}^*\}$.
- Cantor $\Rightarrow$ dois conjuntos finitos têm o mesmo tamanho se os elementos de um conjunto podem ser emparelhados com os elementos do outros conjunto.
  - Método compara os tamanhos sem recorrer à contagem dos elementos.
  - Ideia pode ser estendida para conjuntos infinitos.

Definição 1.6

- Um conjunto $\mathcal{A}$ é contável se é finito ou tem o mesmo tamanho que o conjunto $\mathbb{N}$.

Método da diagonalização

Exemplo 1.7

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- $\mathcal{P} = \{2, 4, 6, \dots\}$.
- Intuitivamente $\mathcal{P}$ parece ser menor que $\mathbb{N}$ ($\mathcal{P} \subset \mathbb{N}$)!
- Segundo a definição de Cantor, $\mathbb{N}$ e $\mathcal{P}$ tem o mesmo tamanho.
- A função $f(n) = 2{\cdot}n + 2$ faz o mapeamento de $\mathbb{N}$ para $\mathcal{P}$:

n	$f(n)$
0	2
1	4
2	6
$\vdots$	$\vdots$

Método da diagonalização

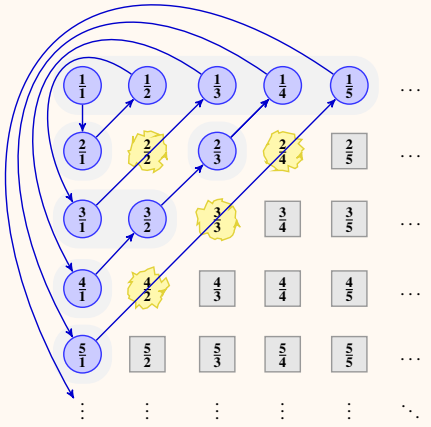
Exemplo 1.8

- $\mathbb{N}^* = \{1, 2, 3, \dots\}$.
- $\mathbb{Q}_+^* = \{\frac{m}{n} \mid m, n \in \mathbb{N}\}$.
- Intuitivamente $\mathbb{Q}_+^*$ parece ser muito maior que $\mathbb{N}^*$!
- Segundo a definição de Cantor, $\mathbb{N}^*$ e $\mathbb{Q}_+^*$ têm o mesmo tamanho.
- Listar todos os elementos de $\mathbb{Q}_+^*$ e corresponder com $\mathbb{N}^*$.
  - $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \cdots, \frac{3}{1}, \frac{3}{2}, \dots$
  - Primeiro da lista com 1, segundo com 2, etc.
  - Problema: elementos da sub-lista $\frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \cdots$ nunca seriam considerados.

Método da diagonalização

Exemplo 1.8

- Correspondência entre $\mathbb{Q}_+^*$ e $\mathbb{N}^*$:



Método da diagonalização

- Quaisquer dois conjuntos infinitos têm o mesmo tamanho?
  - NÃO. Existem conjuntos infinitos que não têm correspondência com $\mathbb{N}$.
  - Tais conjuntos não são contavelmente infinitos.
- Cantor provou que $\mathbb{R}$ não é contavelmente infinito.
  - A prova de Cantor mostra que o intervalo $[0, 1]$ não é contavelmente infinito.
  - Argumento de Diagonalização de Cantor.

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

1. Supor que o intervalo $[0, 1]$ é infinito enumerável.
   - É possível enumerar todos os números deste intervalo como uma seqüência $(r_1, r_2, r_3, \dots)$.
   - Cada um de tais números pode ser representado como uma expansão decimal.

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

2. Arranjar os números em uma lista (eles não precisam estar em ordem).
   - No caso de números com duas expansões decimais, como $0,499\cdots = 0,500\dots$, escolher aquela que acaba com 9's.

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

3. Supor que as expansões decimais do início da seqüência são como segue:

$$\begin{aligned} r_1 &= 0,5105110\dots \\ r_2 &= 0,4132043\dots \\ r_3 &= 0,8245026\dots \\ r_4 &= 0,2330126\dots \\ r_5 &= 0,4107246\dots \\ r_6 &= 0,9937838\dots \\ r_7 &= 0,0105135\dots \\ &\vdots \end{aligned}$$

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

4. Construir um $x \in [0, 1]$, considerando o k-ésimo dígito depois da vírgula da expansão decimal de r_k (dígitos em vermelho):

$$
\begin{aligned}
r_1 &= 0,\mathbf{5}1051110\ldots\\
r_2 &= 0,41\mathbf{1}32043\ldots\\
r_3 &= 0,824\mathbf{5}5026\ldots\\
r_4 &= 0,2330\mathbf{1}126\ldots\\
r_5 &= 0,41072\mathbf{4}46\ldots\\
r_6 &= 0,9937838\ldots\\
r_7 &= 0,0105135\ldots\\
&\vdots
\end{aligned}
$$

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

5. Definir, a partir desses dígitos, os dígitos do número x como:

$$
x_k = \begin{cases} 4 & \text{se o } k\text{-ésimo dígito de } r_k \text{ é } 5,\\ 5 & \text{se o } k\text{-ésimo dígito de } r_k \text{ não é } 5. \end{cases}
$$

   - x_k é o k-ésimo dígito de x.

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

6. Para o exemplo dado, $x = r_k = 0,4555554\ldots$:

$$
\begin{aligned}
r_1 &= 0,\mathbf{5}1051110\ldots\\
r_2 &= 0,41\mathbf{1}32043\ldots\\
r_3 &= 0,824\mathbf{5}5026\ldots\\
r_4 &= 0,2330\mathbf{1}126\ldots\\
r_5 &= 0,41072\mathbf{4}46\ldots\\
r_6 &= 0,9937838\ldots\\
r_7 &= 0,0105135\ldots\\
&\vdots \qquad\qquad \ddots\\
r_k &= \mathbf{0,4555554}\ldots\ \boxed{?}\\
&\vdots
\end{aligned}
$$

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

7. O número x é um número real dentro do intervalo $[0, 1]$.
8. Logo, $x = r_k$ para algum $k \in \mathbb{N}^+$ (supôs-se que $(r_1, r_2, r_3, \ldots)$ enumera todos os números reais no intervalo $[0, 1]$).
9. No entanto, por causa do modo como os dígitos de x foram escolhidos, x difere na k-ésima posição de r_k.

Método da diagonalização

Teorema 1.9

- *O intervalo* $[0, 1]$ *não é contavelmente infinito.*

Demonstração.

10. Logo, x não está na seqüência $(r_1, r_2, r_3, \dots)$.
11. Assim, essa sequência não é uma enumeração do conjunto de todos os reais no intervalo $[0, 1]$ (contradição).
12. Portanto, é falsa a hipótese de que o intervalo $[0, 1]$ é contavelmente finito.

Método da diagonalização

Teorema 1.10

- *O conjunto* $\mathbb{R}$ *não é contavelmente infinito.*

Operações booleanas

Conjunção
$0 \wedge 0 = 0$
$0 \wedge 1 = 0$
$1 \wedge 0 = 0$
$1 \wedge 1 = 1$

Disjunção
$0 \vee 0 = 0$
$0 \vee 1 = 1$
$1 \vee 0 = 1$
$1 \vee 1 = 1$

Negação
$\neg 0 = 1$
$\neg 1 = 0$

OU Exclusivo
$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Implicação
$0 \rightarrow 0 = 1$
$0 \rightarrow 1 = 1$
$1 \rightarrow 0 = 0$
$1 \rightarrow 1 = 1$

Igualdade
$0 \leftrightarrow 0 = 1$
$0 \leftrightarrow 1 = 0$
$1 \leftrightarrow 0 = 0$
$1 \leftrightarrow 1 = 1$

Expressões booleanas

$$
\begin{aligned}
P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R) \\
P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R) \\
P \vee Q &= \neg(\neg P \wedge \neg Q) \\
P \rightarrow Q &= \neg P \vee Q \\
P \leftrightarrow Q &= (P \rightarrow Q) \wedge (Q \rightarrow p) \\
P \oplus Q &= \neg(P \leftrightarrow Q)
\end{aligned}
$$

Teoremas e provas

- Teorema: respostas a questões matemáticas.
  - Se certas condições são verdadeiras, então alguma conclusão também é verdadeira.
  - **Hipótese** verdadeira $\Longrightarrow$ **Tese** verdadeira.
- Instância do teorema:
  - Atribuição particular de valores a variáveis livres nas hipóteses e conclusões.
  - Variáveis livres podem assumir quaisquer valores do universo em discussão.
- Teorema correto:
  - Tese verdadeira para toda instância que torne a hipótese verdadeira.

Teoremas e provas

- Contra-Exemplo
  - Instância que torna a hipótese verdadeira mas leva a uma conclusão falsa.
  - Encontrar um contra-exemplo é suficiente para mostrar que o teorema é falso.
  - Único modo de mostrar que um teorema é verdadeiro é provando-o!

Exemplo 1.11

- `Teorema 1`: Se $x > 3$ e $y < 2$, então $x^2 - 2y > 5$.
  - $x = 5$ e $y = 1 \Rightarrow 23 > 5$: Não prova o teorema, apenas verifica **uma** instância do mesmo.
- `Teorema 2`: Se $x > 3$, então $x^2 - 2{\cdot}y > 5$.
  - $x = 4$ e $y = 6 \Rightarrow x^2 - 2{\cdot}y = 4 > 5$: Contra-exemplo!

Teoremas e provas

- A prova é um argumento dedutivo cujas premissas são as hipóteses e cuja conclusão é a tese do teorema.
  - Argumento válido.
  - Forma lógica das hipóteses $\Rightarrow$ forma lógica da conclusão.
- Qual a estratégia de prova mais adequada às várias formas de hipóteses e teses?

Teoremas e provas

- Regras básicas:
  - Nunca afirme alguma coisa se você não puder justificá-la completamente.
  - Se você tem qualquer dúvida a respeito da justificativa para uma afirmação, então ela não é adequada.
  - Se o seu raciocínio não o convence, como convencerá a outros?

Teoremas e provas

- Supor e Afirmar
  - **Afirmar** um enunciado é alegar que o mesmo é verdadeiro e isso não é aceitável em uma prova, a menos que possa ser justificado.
  - **Supor** um enunciado permite dizer o que poderia ser verdadeiro se o enunciado fosse verdadeiro.

Transformação do problema

- Provar uma conclusão da forma $P \to Q$
  a) Adicione P à lista de hipóteses.
  b) Mude a conclusão de $P \to Q$ para Q.
  - Se resolver o novo problema, na verdade terá mostrado que se P é verdadeiro então Q também é verdadeiro, ou seja, terá resolvido o problema original $P \to Q$.
- Notação:
  - Dados: enunciados conhecidos ou aqueles que se assumiu serem verdadeiros em algum ponto da demonstração.
  - Objetivo: enunciados a serem provados.

Teoremas e provas

- Provar uma conclusão da forma $P \to Q$:
  a) Suponha que P é verdadeiro.
  b) Use este postulado para concluir que Q é verdadeiro.

Exemplo 1.12

- Sejam $a, b \in \mathbb{R}$. Prove que se $0 < a < b$, então $a^2 < b^2$.
  - Dados: $a, b \in \mathbb{R}$ (hipótese).
  - Objetivo: Se $0 < a < b$, então $a^2 < b^2$ (tese).

  $\Downarrow$
  - Dados: $a, b \in \mathbb{R}$, $0 < a < b$.
  - Objetivo: $a^2 < b^2$.

Provar um "Objetivo" da forma $P \to Q$

- Rascunho:

Dados	Objetivo
$\vdots$	$P \to Q$
$\vdots$ P	Q

Antes da transformação.

Depois da transformação.

- Solução:

  Suponha que P é verdadeiro.
  [`Prove que` Q `é verdadeiro`]
  Portanto, $P \to Q$.

"Objetivo" da forma $P \to Q \equiv \neg Q \to \neg P$

- Rascunho:

Dados	Objetivo
$\vdots$	$P \to Q$
$\vdots$ $\neg Q$	$\neg P$

Antes da transformação.

Depois da transformação.

- Solução:

  Suponha que Q é falso.

  [`Prove que` $\neg P$ `é verdadeiro`]

  Portanto, $P \to Q$.

"Objetivo" da forma $P \to Q \equiv \neg Q \to \neg P$

Exemplo 1.13

- Sejam $a, b, c \in \mathbb{R}$ e tais que $a > b$. Prove que se $a{\cdot}c \leqslant b{\cdot}c$, então $c < 0$.

Dados	Objetivo
$a, b, c \in \mathbb{R}$ $a > b$	$a{\cdot}c \leqslant b{\cdot}c \Rightarrow c \leqslant 0$
$a, b, c \in \mathbb{R}$ $a > b$ $c > 0$	$a{\cdot}c > b{\cdot}c$

- Solução:

  Suponha $c > 0$. Multiplicando ambos os lados da desigualdade $a > b$ por c conclui-se que $a{\cdot}c > b{\cdot}c$. Portanto, se $a{\cdot}c \leqslant b{\cdot}c$ então $c \leqslant 0$.

"Objetivo" da forma $\neg P$

- Se possível, reescreva o objetivo de alguma outra forma (enunciado positivo) e use uma das estratégias de prova.

Exemplo 1.14

- Sejam os conjuntos $A, B, C \subseteq \mathbb{U}$. Suponha que $A \cap C \subseteq B$ e $a \in C$. Prove que $a \notin A \backslash B$.
- Rascunho:

Dados	Objetivo
$A, B, C \subseteq \mathbb{U}$ $A \cap C \subseteq B$ $a \in C$	$a \notin A \backslash B$

"Objetivo" da forma $\neg P$

- Se possível, reescreva o objetivo de alguma outra forma (enunciado positivo) e use uma das estratégias de prova.

Exemplo 1.14

- Obs-1:

$$P \to Q \equiv \neg P \vee Q \equiv \neg(P \wedge \neg Q)$$

- Obs-2:

$$\begin{array}{lcll} a \notin A \backslash B & \equiv & \neg(a \in A \wedge a \notin B) & \text{[Definição de } A \backslash B\text{]} \\ & \equiv & a \notin A \vee a \in B & \text{[DeMorgan]} \\ & \equiv & a \in A \Rightarrow a \in B & \text{[Condicional]} \end{array}$$

“Objetivo” da forma $\neg P$

- Se possível, reescreva o objetivo de alguma outra forma (enunciado positivo) e use uma das estratégias de prova.

Exemplo 1.14

- Rascunho:

Dados	Objetivo
$A, B, C \subseteq \mathbb{U}$ $A \cap C \subseteq B$ $a \in C$	$a \notin A \backslash B$
$A, B, C \subseteq \mathbb{U}$ $A \cap C \subseteq B$ $a \in C$	$a \in A \Rightarrow a \in B$
$A, B, C \subseteq \mathbb{U}$ $A \cap C \subseteq B$ $a \in C$ $a \in A$	$a \in B$

“Objetivo” da forma $\neg P$

- Nem sempre um objetivo da forma $\neg P$ pode ser reescrito como “enunciado positivo”.
- Rascunho:

Dados	Objetivo
$\vdots$	$\neg P$
$\vdots$ P	⟨Contradição⟩

- Solução:

  Suponha que P é verdadeiro.
  [`Prove a contradição`]
  Portanto, P é falso.

“Objetivo” da forma $\neg P$

- Prova por contradição:
  - Vantagem: supor P verdadeiro permite crescer a lista de hipóteses.
  - Desvantagem: Objetivo vago, ou seja, produzir uma contradição de alguma coisa que é verdadeiro.

“Objetivo” da forma $\neg P$

Exemplo 1.15

- Dados $x, y \in \mathbb{R}$, prove que se $x^2 + y = 13$ e $y \neq 4$ então $x \neq 3$.
  - $x \neq 3 \equiv \neg(x = 3)$, logo estratégia anterior não pode ser usada.

Dados	Objetivo
$x, y \in \mathbb{R}$	$x^2 + y = 13$ e $y \neq 4 \Rightarrow x \neq 3$
$x, y \in \mathbb{R}$ $x^2 + y = 13$ $y \neq 4$	$x \neq 3$
$x, y \in \mathbb{R}$ $x^2 + y = 13$ $y \neq 4$ $x = 3$	⟨Contradição⟩

Usar um "Dado" da forma $\neg P$

- Numa prova por contradição tente fazer de P o objetivo.
  - Se P pode ser provado, P contradiz o dado $\neg P$.

Dados	Objetivo
$\vdots$ $\neg P$	⟨Contradição⟩
$\vdots$ $\neg P$	P

- Solução:

  [`Prove que` P `é verdadeiro`]
  Como já se sabe que $\neg P$ é verdadeiro, tem-se uma contradição.

Provas por contradição

- Provas por contradição podem ser usadas com objetivos que não são da forma $\neg P$.

Exemplo 1.16

- Dados $A, B, C \subseteq \mathbb{U}$, tais que $A \backslash B \subseteq C$, se $x \in A \backslash C$, então $x \in B$.

Dados	Objetivo	Solução
$A \backslash B \subseteq C$	$x \in A \backslash C \Rightarrow x \in B$	
$A \backslash B \subseteq C$ $x \in A \backslash C$	$x \in B$	Suponha $x \in A \backslash C$. [`Prove que` $x \in B$]. Portanto, se $x \in A \backslash C$, então $x \in B$.
$A \backslash B \subseteq C$ $x \in A \backslash C$ $x \notin B$	⟨Contradição⟩	Suponha $x \in A \backslash C$. Suponha $x \notin B$. [`Prove a contradição`]. Assim, $x \in B$. Portanto, se $x \in A \backslash C$, então $x \in B$.
$A \backslash B \subseteq C$ $x \in A$ $x \notin C$ $x \notin B$	$x \in C$	Suponha $x \in A \backslash C$ ($x \in A$ e $x \notin C$). Suponha $x \notin B$. [`Prove que` $x \in C$]. Isto contradiz o fato de $x \notin C$. Assim, $x \in B$. Portanto, se $x \in A \backslash C$, então $x \in B$.

"Dado" da forma $P \to Q$

- Se P é dado também ou se é possível provar que P é verdadeiro, conclua que Q é verdadeiro.
  - Se P e $P \to Q$ são verdadeiros, então Q também é verdadeiro.
  - Se $P \to Q$ é verdadeiro e Q é falso, então P deve ser falso também.

"Dado" da forma $P \to Q$

Exemplo 1.17

- Suponha $P \to (Q \to R)$. Prove que $\neg R \to (P \to \neg Q)$.
  - $P \to Q \equiv \neg Q \to \neg P$.

Dados	Objetivo	Solução
$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$	
$P \to (Q \to R)$ $\neg R$	$P \to \neg Q$	Suponha $\neg R$. [`Prove que` $P \to \neg Q$]. Portanto, $\neg R \to (P \to \neg Q)$.
$P \to (Q \to R)$ $\neg R$ P	$\neg Q$	Suponha $\neg R$. Suponha P. [`Prove` $\neg Q$]. Portanto, $P \to \neg Q$. Portanto, $\neg R \to (P \to \neg Q)$.
$P \to (Q \to R)$ $\neg R$ P $Q \to R$	$\neg Q$	Suponha $\neg R$. Suponha P. De P e $P \to (Q \to R)$, segue que $Q \to R$. [`Prove` $\neg Q$]. Portanto, $P \to \neg Q$. Portanto, $\neg R \to (P \to \neg Q)$.

Provas por contradição

Exemplo 1.18

- Sejam $A, B \subseteq \mathbb{U}$ e tais que $A \subset B$. Considere elementos genéricos a e b tais que $a \in A$ e a e b não pertencem ao mesmo tempo a B. Prove que $b \notin B$.

Dados	Objetivo	Solução
$A \subset B$ $a \in A$ $\neg(a \in B \wedge b \in B)$	$b \notin B$	
$A \subset B$ $a \in A$ $a \in B \rightarrow b \notin B$	$b \notin B$	
$A \subset B$ $a \in A$ $a \in B \rightarrow b \notin B$	$a \in B$	

Provar um "Objetivo" da forma $\forall\, x\, P(x)$

- Considere x um objeto arbitrário e prove $P(x)$.
- Rascunho:

Dados	Objetivo
$\vdots$	$\forall\, x\, P(x)$
$\vdots$ x arbitrário	$P(x)$

- Solução:
  Considere um x arbitrário.
  [Prove $P(x)$].
  Como x é arbitrário, conclui-se que $\forall\, x\, P(x)$.

Provar um "Objetivo" da forma $\forall\, x\, P(x)$

Exemplo 1.19

- Sejam $A, B \subseteq \mathbb{U}$. Prove que se $A \cap B = A$, então $A \subseteq B$.
- Rascunho:

Dados	Objetivo	Solução
$A, B \subseteq \mathbb{U}$	$A \cap B = A \Rightarrow A \subseteq B$	Suponha $A \cap B = A$.
$A, B \subseteq \mathbb{U}$ $A \cap B = A$	$A \subseteq B$	Considere um $x \in A$ arbitrário. [Prove que $x \in B$].
$A, B \subseteq \mathbb{U}$ $A \cap B = A$	$\forall\, x\, (x \in A \rightarrow x \in B)$	Portanto, $x \in A \rightarrow x \in B$ Como x é arbitrário, conclui-se que
$A, B \subseteq \mathbb{U}$ $A \cap B = A$ $x \in A$	$x \in B$	$\forall\, x\, (x \in A \rightarrow x \in B)$. Assim, $A \subseteq B$. Portanto, se $A \cap B = A$, então $A \subseteq B$.

Provar um "Objetivo" da forma $\exists\, x\, P(x)$

- Tente encontrar um valor de x para o qual você acredita que $P(x)$ seria verdadeiro e prove $P(x)$ para este x.
- Rascunho:

Dados	Objetivo
$\vdots$	$\exists\, x\, P(x)$
$\vdots$ $x = \square$	$P(x)$

- Solução:
  Seja $x = \square$.
  [Prove $P(x)$].
  Portanto, $\exists\, x\, P(x)$.

Provar um "Objetivo" da forma $\exists\, x\, P(x)$

Exemplo 1.20

- Prove que para todo número real x, se $x > 0$ então existe um número real y tal que $y{\cdot}(y+1) = x$.
- Rascunho:

Dados	Objetivo
$x \in \mathbb{R}$	$\forall\, x\, (x > 0) \Rightarrow \exists\, y\, (y{\cdot}(y+1) = x)$
$x > 0$	$\exists\, y\, (y{\cdot}(y+1) = x)$
$x > 0$	$y{\cdot}(y+1) = x$
$y = \frac{-1+\sqrt{1+4{\cdot}x}}{2}$	

- Solução:

  Suponha um número real arbitrário $x > 0$. Seja $y = \frac{-1+\sqrt{1+4{\cdot}x}}{2}$. [`Prove` que $y{\cdot}(y+1) = x$]. Logo, $\exists\, y\, (y{\cdot}(y+1) = x)$. Assim, $x > 0 \Rightarrow \exists\, y\, (y{\cdot}(y+1) = x)$. Portanto, como x é arbitrário, conclui-se que $\forall\, x\, (x > 0) \Rightarrow \exists\, y\, (y{\cdot}(y+1) = x)$.

Técnicas gerais

- Provar um objetivo da forma $P \wedge Q$.
  - Prove P e Q separadamente.
- Usar um "Dado" da forma $P \wedge Q$.
  - Trate P e Q como "dados" separados.
- Provar um objetivo da forma $P \leftrightarrow Q$.
  - Prove $P \rightarrow Q$ e $Q \rightarrow P$ separadamente.
- Usar um "Dado" da forma $P \leftrightarrow Q$.
  - Trate como dois "dados" separados: $P \rightarrow Q$ e $Q \rightarrow P$.

Exemplos de demonstrações

Exemplo 1.21

- Dados $A, B, C \subseteq \mathbb{U}$ tais que $A \subseteq B$ e A e C são disjuntos, prove que $A \subseteq B \backslash C$.
- Rascunho:

Dados	Objetivo
$A \subseteq B$ $A \cap C = \varnothing$	$A \subseteq B \backslash C$
$A \subseteq B$ $A \cap C = \varnothing$	$\forall\, x\, (x \in A \Rightarrow x \in B \backslash C)$
$A \subseteq B$ $A \cap C = \varnothing$ $x \in A$	$x \in B \backslash C$
$A \subseteq B$ $A \cap C = \varnothing$ $x \in A$	$x \in B$ $x \notin C$

Exemplos de demonstrações

Exemplo 1.22

- Prove que $\forall\, x\, \neg P(x) \Leftrightarrow \neg\exists\, x\, P(x)$.
- Rascunho:

$\Longrightarrow$

Dados	Objetivo
$\forall\, x\, \neg P(x)$	$\neg\exists\, x\, P(x)$
$\forall\, x\, \neg P(x)$ $\exists\, x\, P(x)$	$\langle$Contradição$\rangle$

$\Longleftarrow$

Dados	Objetivo
$\neg\exists\, x\, P(x)$	$\forall\, x\, \neg P(x)$
$\neg\exists\, x\, P(x)$ x arbitrário	$\neg P(x)$
$\neg\exists\, x\, P(x)$ x arbitrário $P(x)$	$\langle$Contradição$\rangle$

Exemplos de demonstrações

Exemplo 1.23

- Dados $A, B, C \subseteq \mathbb{U}$, prove que $A \cap (B \backslash C) = (A \cap B) \backslash C$.

$$\begin{aligned} A \cap (B \backslash C) = (A \cap B) \backslash C &\equiv [A \cap (B \backslash C) \subseteq (A \cap B) \backslash C] \wedge \\ &\quad [(A \cap B) \backslash C \subseteq A \cap (B \backslash C)] \\ &\equiv \forall\, x\, ((x \in A \cap (B \backslash C) \Leftrightarrow x \in (A \cap B) \backslash C) \end{aligned}$$

- Rascunho:

	Dados	Objetivo
$\Longrightarrow$	$x \in A \cap (B \backslash C)$	$x \in (A \cap B) \backslash C$
$\Longleftarrow$	$x \in (A \cap B) \backslash C$	$x \in A \cap (B \backslash C)$

Indução matemática

- Provar um objetivo da forma $\forall\, n \in \mathbb{N}\ P(n)$.
- Rascunho:
  - Prove $P(0)$.
  - Prove que $\forall\, n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)$.
- Exercícios:
  - Prove que $\forall\, n \in \mathbb{N},\ n \geqslant 5,\ P(2^n > n^2)$.
  - Prove que $\forall\, n \in \mathbb{N},\ P(3 \mid (n^3 - n))$.

Dados	Objetivo
$n \in \mathbb{N}$	$\exists\, j \in \mathbb{Z}\ (3.j = (n+1)^3 - (n+1))$
$\exists\, k \in \mathbb{Z}\ (3.k = n^3 - n)$	

Indução forte

- Provar um objetivo da forma $\forall\, n \in \mathbb{N},\ P(n)$.
  - Prove que $\forall\, n\, [(\forall\, k < n\ P(k)) \Rightarrow P(n)],\ \ n, k \in \mathbb{N}$.
- Rascunho:
  - Suponha que n é um número natural arbitrário ($n \in \mathbb{N}$).
  - Suponha que $\forall\, k < n\ P(k)$.
  - Prove $P(n)$.
- Obs: Não é necessário provar o caso base.
  - Suponha que se tenha provado $\forall\, n\, [(\forall\, k < n\ P(n)) \Rightarrow P(n+1)],\ \ n, k \in \mathbb{N}$.
  - Se $n = 0$, conclui-se que $\forall\, k < 0\ P(k) \Rightarrow P(0)$.
  - Pode-se concluir que $P(0)$ é verdadeiro.

Provas por indução

Elemento mínimo

- Dado um subconjunto não vazio $S \subseteq \mathbb{N}$, o elemento mínimo de S é um elemento $x_0 \in S$ tal que $x_0 \leqslant x,\ \forall\, x \in S$.
  - $\min S = x_0 \Leftrightarrow x_0 \in S$ e $x_0 \leqslant x,\ \forall\, x \in S$.

Princípio da boa ordenação

- Todo subconjunto não vazio $S \subseteq \mathbb{N}$ possui um elemento mínimo.
  - $\forall\, S \subseteq \mathbb{N},\ S \neq \varnothing \Rightarrow \exists\, \min S$.

Provas por indução

Teorema 1.24 (Princípio da indução finita)

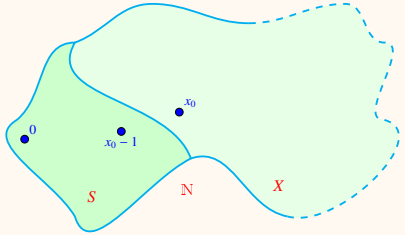
- *Seja $S \subseteq \mathbb{N}$ que satisfaz as seguintes condições:*
  i. $0 \in S$; *e*
  ii. *para todo inteiro positivo k, se $k \in S$, então $k + 1 \in S$.*

  Neste caso, S é o próprio conjunto $\mathbb{N}$, ou seja, $S = \mathbb{N}$.

Provas por indução

Demonstração.

- Supor, por absurdo, que $S \neq \mathbb{N}$.
- Seja X o conjunto de todos os inteiros que não pertencem a S:
  - $X = \{x \mid x \in \mathbb{N} \text{ e } x \notin S\} = \mathbb{N} - S$.
- X é subconjunto não vazio de $\mathbb{N}$ ($\varnothing \neq X \subset \mathbb{N}$) e, pelo "Princípio da Boa Ordenação", existe um elemento mínimo x_0 de X ($\min X$).



Provas por indução

Demonstração.

- Pela condição i, $0 \in S$, de modo que $x_0 > 0$ e, portanto, $x_0 - 1 \notin X$.
- Como $x_0 - 1 \in S$, pela condição ii, $(x_0 - 1) + 1 = x_0 \in S$.
- Dada a contradição ($x_0 = \min X$ e $X = \mathbb{N} - S$, ou seja, $x_0 \notin S$), concluí-se que $X = \varnothing$ e $S = \mathbb{N}$.
- O único subconjunto de $\mathbb{N}$ que satisfaz as condições i e ii é o próprio $\mathbb{N}$.

Provas por indução

Teorema 1.25 (Princípio da indução matemática)

- *Seja $P(n)$ uma proposição associada a inteiros $n \geqslant 0$ e que satisfaz as seguintes condições:*
  1. *a proposição $P(0)$ é verdadeira; e*
  2. *para todo inteiro positivo k, se a proposição $P(k)$ é verdadeira, então a proposição $P(k + 1)$ também é verdadeira.*

  Neste caso, a proposição $P(n)$ é verdadeira para todo inteiro $n \geqslant 0$.

Provas por indução

Demonstração.

- Seja S o conjunto de todos os inteiros para os quais a proposição $P(n)$ é verdadeira.
  - $S = \{n \in \mathbb{N} \mid P(n) \text{ é verdadeira}\}$.
- Pela condição 1, $P(0)$ é verdadeira e, portanto, $0 \in S$.
- Pela condição 2, para todo inteiro positivo k, $P(k)$ verdadeira ($k \in S$) implica que $P(k+1)$ é verdadeira ($k+1 \in S$).
- O conjunto S satisfaz às condições i e ii do "Princípio da Indução Finita" e, portanto, $S = \mathbb{N}$.
- A proposição $P(n)$ é verdadeira para todo inteiro $n \geqslant 0$.

□

Provas por indução

Exemplo 1.26

- Todos os inteiros da forma $8^n - 2^n$ são divisíveis por 6, para $n \in \mathbb{N}^+$.
- Seja $P(n)$ a proposição: $8^n - 2^n$ é divisível por 6, para $n \in \mathbb{N}^+$.
- Seja $S = \{k \in \mathbb{N}^+ \mid P(n) \text{ é verdadeira.}\}$.
- Objetivo: provar que $S = \mathbb{N}^+$!

Provas por indução

Exemplo 1.26

Base: $1 \in S$, pois $P(1)$ é verdadeira ($8^1 - 2^1 = 6$).

H. I.: Suponha que $1 < k \in S$, ou seja, $P(k)$ é verdadeira.

Provas por indução

Exemplo 1.26

P. I.: $k+1 \in S$, ou seja, $P(k+1)$ é verdadeira:

$$\begin{aligned} 8^{k+1} - 2^{k+1} &= 8 \cdot 8^k - 2 \cdot 2^k \\ &= 8 \cdot 8^k - 2 \cdot 2^k + 8 \cdot 2^k - 8 \cdot 2^k \\ &= 8 \cdot (8^k - 2^k) + 2^k \cdot (8 - 2) \\ &= 8 \cdot (8^k - 2^k) + 2^k \cdot (6) \end{aligned}$$

Por hipótese de indução, $(8^k - 2^k)$ é divisível por 6.

Logo, $S = \mathbb{N} - \{0\}$ e a proposição $P(n)$ é verdadeira para todo $n \geqslant 1$.

Indução matemática

Exemplo 1.27

- Para todo inteiro n maior que 3, $n! > 2^n$.
- Seja $P(n)$ a proposição: $n! > 2^n$, para todo $4 \leqslant n \in \mathbb{N}$.
- Seja $S = \{n \in \mathbb{N} \mid P(n)$ é verdadeira.$\}$.
- Objetivo: provar que $S = \mathbb{N} - \{0, 1, 2, 3\}$!

Indução matemática

Exemplo 1.27

Base: Para $n = 4$, $4! = 24 > 16 = 2^4$. Logo, $4 \in S$.

H. I.: Suponha que um certo $4 \leqslant n = k \in S$, ou seja, $k! > 2^k$ e $n = k \in S$.

Indução matemática

Exemplo 1.27

P. I.: Deve-se mostrar que $n = k + 1 \in S$, ou seja, $P(k + 1)$ é verdadeira:

$$\begin{array}{rcll} (k+1)! & = & (k+1) \cdot k! & \\ & > & (k+1) \cdot 2^k & \text{(hipótese indutiva)} \\ & > & 2 \cdot 2^k & \text{(já que } k+1 > 2) \\ & = & 2^{k+1} & \end{array}$$

Dado que $(k + 1)! > 2^{k+1}$, $P(n)$ é verdadeira para todo $n \in \mathbb{N} - \{0, 1, 2, 3\}$, ou seja, $S = \mathbb{N} - \{0, 1, 2, 3\}$.

Livros texto


R. P. Grimaldi
Discrete and Combinatorial Mathematics – An Applied Introduction.
Addison Wesley, 1994.


D. J. Velleman
How To Prove It – A Structured Approach.
Cambridge University Press, 1996.


J. E. Hopcroft; J. Ullman.
Introdução Ã Teoria de Autômatos, Linguagens e Computação.
Ed. Campus.


T. A. Sudkamp.
Languages and Machines – An Introduction to the Theory of Computer Science.
Addison Wesley Longman, Inc. 1998.


J. Carroll; D. Long.
Theory of Finite Automata – With an Introduction to Formal Languages.
Prentice-Hall, 1989.


M. Sipser.
Introduction to the Theory of Computation.
PWS Publishing Company, 1997.


H. R. Lewis; C. H. Papadimitriou
Elementos de Teoria da Computação.
Bookman, 2000.