Soluções dos Exercícios Propostos no Livro

Introdução aos Fundamentos da Computação: Linguagens e Máquinas

(Ed. Thomson, 2006)

Newton José Vieira
Departamento de Ciência da Computação
Instituto de Ciências Exatas
Universidade Federal de Minas Gerais

Belo Horizonte, 30/06/2007

Peço a quem encontrar erros nas soluções a seguir entrar em contato com o autor no endereço nvieira@dcc.ufmg.br. Antecipadamente, agradeço

Capítulo 1

Conceitos Preliminares

1.1 Representação

Nesta seção não há exercícios.

1.2 Prova de Teoremas

1. a) A afirmativa $(\alpha \wedge \beta) \rightarrow \alpha$ só é falsa se $\alpha \wedge \beta$ é verdadeira e α é falsa. Mas a $\alpha \wedge \beta$ não pode ser verdadeira se α é falsa. Assim, $(\alpha \wedge \beta) \rightarrow \alpha$ não pode ser falsa; logo, é válida.

   b) A afirmativa $\alpha \rightarrow (\alpha \vee \beta)$ só é falsa se α é verdadeira e $\alpha \vee \beta$ é falsa. Mas, sendo α verdadeira, $\alpha \vee \beta$ não pode ser falsa. Assim, $\alpha \rightarrow (\alpha \vee \beta)$ não pode ser falsa; logo, é válida.

   c) A afirmativa $(\alpha \wedge \neg\alpha) \rightarrow \beta$ só pode ser falsa se $\alpha \wedge \neg\alpha$ é verdadeira e β é falsa. Mas a afirmativa $\alpha \wedge \neg\alpha$ não pode ser verdadeira, pois é uma contradição. Assim, $(\alpha \wedge \neg\alpha) \rightarrow \beta$ não pode ser falsa; logo, é válida.

   d) A afirmativa $\alpha \rightarrow (\beta \vee \neg\beta)$ só é falsa se α é verdadeira e $\beta \vee \neg\beta$ é falsa. Mas, $\beta \vee \neg\beta$ não pode ser falsa, pois β e $\neg\beta$ não podem ser ambas falsas. Assim, $\alpha \rightarrow (\beta \vee \neg\beta)$ não pode ser falsa; logo, é válida.

   e) A afirmativa $(\alpha \rightarrow \beta) \vee \alpha$ só pode ser falsa se ambas, $\alpha \rightarrow \beta$ e α são falsas. Mas, sendo α falsa, $\alpha \rightarrow \beta$ é verdadeira. Assim, $(\alpha \rightarrow \beta) \vee \alpha$ não pode ser falsa; logo, é válida.

   f) A afirmativa $(\alpha \rightarrow \beta) \vee (\beta \rightarrow \alpha)$ só pode ser falsa se $\alpha \rightarrow \beta$ e $\beta \rightarrow \alpha$ são falsas. Para $\alpha \rightarrow \beta$ ser falsa, α deve ser verdadeira (e β falsa), e para $\beta \rightarrow \alpha$ ser falsa, α deve ser falsa (e β verdadeira); contradição! Assim, a afirmativa original não pode ser falsa; logo, é válida.

2. a) Suponha que $\alpha \rightarrow \beta$ é verdadeira. Segue-se que α é falsa ou β é verdadeira. No primeiro caso, $\neg\alpha$ é verdadeira e, portanto, $\neg\beta \rightarrow \neg\alpha$ é verdadeira. No segundo caso, $\neg\beta$ é falsa e, portanto, $\neg\beta \rightarrow \neg\alpha$ é também verdadeira. Logo, $(\alpha \rightarrow \beta) \Rightarrow (\neg\beta \rightarrow \neg\alpha)$. Suponha, por outro lado, que $\alpha \rightarrow \beta$ é falsa. Segue-se que α é verdadeira e β é falsa. Com isto, $\neg\alpha$ é falsa e $\neg\beta$ é verdadeira e, portanto, $\neg\beta \rightarrow \neg\alpha$ é falsa. Logo, $(\neg\alpha \rightarrow \neg\beta) \Rightarrow (\alpha \rightarrow \beta)$.

   b) Primeiro, mostra-se que $(\alpha \vee \beta) \rightarrow \gamma \Rightarrow [(\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)]$: Suponha que $(\alpha \vee \beta) \rightarrow \gamma$ é verdadeira. Segue-se que $\alpha \vee \beta$ é falsa ou γ é verdadeira. No primeiro caso, α e β são falsas e, portanto, $\alpha \rightarrow \gamma$ e $\beta \rightarrow \gamma$ são verdadeiras. No segundo caso, sendo

γ verdadeira, $\alpha \to \gamma$ e $\beta \to \gamma$ são também verdadeiras. Assim, se $(\alpha \vee \beta) \to \gamma$ é verdadeira, $(\alpha \to \gamma) \wedge (\beta \to \gamma)$ é verdadeira. Logo, $(\alpha \vee \beta) \to \gamma \Rightarrow [(\alpha \to \gamma) \wedge (\beta \to \gamma)]$. Resta mostrar que $[(\alpha \to \gamma) \wedge (\beta \to \gamma)] \Rightarrow (\alpha \vee \beta) \to \gamma$. Para isto, suponha que $(\alpha \to \gamma) \wedge (\beta \to \gamma)$ é verdadeira; segue-se que $\alpha \to \gamma$ e $\beta \to \gamma$ são verdadeiras. Destas duas segue-se que γ é verdadeira ou α e β são falsas, e, neste último caso, $\alpha \vee \beta$ é falsa. Mas, sendo γ verdadeira ou $\alpha \vee \beta$ falsa, $(\alpha \vee \beta) \to \gamma$ é verdadeira. Portanto, $[(\alpha \to \gamma) \wedge (\beta \to \gamma)] \Rightarrow (\alpha \vee \beta) \to \gamma$.

c) Suponha que $\alpha \to (\beta \wedge \gamma)$ é verdadeira. Segue-se que α é falsa ou $\beta \wedge \gamma$ é verdadeira. No primeiro caso, sendo α falsa, $\alpha \to \beta$ e $\alpha \to \gamma$ são verdadeiras. No segundo caso, sendo β verdadeira, $\alpha \to \beta$ é verdadeira, e sendo γ verdadeira, $\alpha \to \gamma$ é verdadeira. Logo, $(\alpha \to (\beta \wedge \gamma)) \Rightarrow ((\alpha \to \beta) \wedge (\alpha \to \gamma))$. Suponha, agora, que $\alpha \to (\beta \wedge \gamma)$ é falsa. Segue-se que α é verdadeira e $(\beta \wedge \gamma)$ é falsa, ou seja, β é falsa ou γ é falsa. Com isto, $\alpha \to \beta$ é falsa ou $\alpha \to \gamma$ é falsa e, portanto, $(\alpha \to \beta) \wedge (\alpha \to \gamma)$ é falsa. Logo, $(\alpha \to \beta) \wedge (\alpha \to \gamma) \Rightarrow \alpha \to (\beta \wedge \gamma)$.

3. a) Não existe atribuição de valor-verdade para α tal que ambas, α e $\neg\alpha$ sejam verdeiras. Assim, *por vacuidade*, sempre α e $\neg\alpha$ são verdadeiras, γ também é.

   b) Se $\alpha \to \gamma$ é verdadeira, então α é falsa ou γ é verdadeira. No primeiro caso, $\alpha \wedge \beta$ é falsa e, portanto, $(\alpha \wedge \beta) \to \gamma$ é verdadeira. No segundo caso, sendo γ é verdadeira, $(\alpha \wedge \beta) \to \gamma$ é também verdadeira. Conclui-se, então que $\{\alpha \to \gamma\} \Rightarrow (\alpha \wedge \beta) \to \gamma$.

   c) Suponha que $\neg\alpha \to \beta$ e $\neg\beta$ sejam verdadeiras. Neste caso, β é falsa e, portanto, $\neg\alpha$ é falsa. Sendo $\neg\alpha$ falsa, α é verdadeira. Logo, se $\neg\alpha \to \beta$ e $\neg\beta$ são verdadeiras, α é verdadeira, ou seja, $\{\neg\alpha \to \beta, \neg\beta\} \Rightarrow \alpha$.

4. Sejam x e y números reais tais que $x > 0$ e $x < y$. Destas duas últimas segue-se que $x^2 < xy$. Das mesmas, segue-se também que $y > 0$. Desta e do fato de que $x < y$, deduz-se que $xy < y^2$. De $x^2 < xy$ e $xy < y^2$, conclui-se que $x^2 < y^2$.

5. Sejam x e y números reais arbitrários. Suponha que $x^2 + y = 13$ e $y \neq 4$. Deve-se mostrar que, neste caso, $x \neq 3$. Suponha o contrário: $x = 3$. Então, substituindo-se x por 3 em $x^2 + y = 13$, obtém-se: $3^2 + y = 13$ e, assim, $y = 13 - 9 = 4$. Contradição. Logo, se $x^2 + y = 13$ e $y \neq 4$, então $x \neq 3$.

6. Seja x um número real tal que $x > 2$. Seja $k = (x + \sqrt{x^2 - 4})/2$; observe que k é um número real, pois $x > 2$. Além disso,

$$k + \frac{1}{k} = \frac{x + \sqrt{x^2 - 4}}{2} + \frac{1}{(x + \sqrt{x^2 - 4})/2} = \frac{x + \sqrt{x^2 - 4}}{2} + \frac{2}{x + \sqrt{x^2 - 4}}.$$

Fazendo-se as operações e simplificando-se obtém-se:

$$k + \frac{1}{k} == \frac{x^2 + 2x\sqrt{x^2 - 4} + x^2 - 4 + 4}{2x + 2\sqrt{x^2 - 4}} = x.$$

Conclui-se, então, que para todo número real x, se $x > 2$, existe um número y tal que $y + (1/y) = x$.

7. Seja x um número natural. A prova será feita pela contrapositiva. Suponha, assim, que $\sqrt{x}$ é um número racional. Neste caso, $\sqrt{x} = p/q$, onde p e q são números naturais primos entre si. Segue-se que $x = p^2/q^2$. Como p e q são primos entre si, p^2 e q^2 são primos entre si, e como x é um número natural q^2 só pode ser 1 e $x = p^2$. Portanto, para todo número natural x, se x não é é um quadrado perfeito, $\sqrt{x}$ não é um número racional.

8. Seja n um número inteiro não divisível por 3. Então $n = 3q + r$, onde q é um inteiro e $r \in \{1, 2\}$. Caso 1: $r = 1$. Tem-se que $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. Fazendo-se $k = 3q^2 + 2q$ tem-se que k é um inteiro tal que $n^2 = 3k + 1$, como requerido. Caso 2: $r = 2$. Tem-se que $n^2 = (3q+2)^2 = 9q^2+12q+4 = 3(3q^2+4q+1)+1$. Fazendo-se $k = 3q^2 + 4q + 1$ tem-se que k é um inteiro tal que $n^2 = 3k + 1$.

1.3 Conjuntos

1. a) $A \cap B = \{0, 1, 2, 3, 4, 5\}$.
   b) $C = \{-4, -2, 0, 2, 4, 6, 8\}$.
   c) $D = \{-5, -4, -3, -2, -1, 6, 7, 8\}$.
   d) $\{(0, 7), (2, 7), (4, 7)\}$.

2. Resposta para a primeira pergunta: $A - B = B - A$ se, e somente se, $A = B$. Prova:

   ($\leftarrow$) Suponha que $A = B$. Então $A - B = B - A = \emptyset$.

   ($\rightarrow$) Suponha que $A - B = B - A$. Para provar, primeiramente, que $A \subseteq B$, seja $x \in A$. Suponha que $x \notin B$. Neste caso, $x \in A - B$, e, como $A - B = B - A$, $x \in B - A$. Mas, neste caso, $x \in B$ e $x \notin A$. Contradição. Assim, se $x \in A$, então $x \in B$, ou seja, $A \subseteq B$. Prova-se que $B \subseteq A$ de forma análoga.

   Resposta para a segunda pergunta: $A \cup B = A \cap B$ se, e somente se, $A = B$. Prova:

   ($\leftarrow$) Suponha que $A = B$. Então $A \cup B = A \cap B = A = B$.

   ($\rightarrow$) Suponha que $A \cup B = A \cap B$. Para provar, primeiramente, que $A \subseteq B$, seja $x \in A$. Com isto, $x \in A \cup B$. Neste caso, como $A \cup B = A \cap B$, $x \in A \cap B$. Assim $x \in B$. Portanto, se $x \in A$, então $x \in B$, ou seja, $A \subseteq B$. Prova-se que $B \subseteq A$ de forma análoga.

3. Será mostrado que $A \cup B = A \cup C$ se, e somente se, $(B - C) \cup (C - B) \subseteq A$. (Ou seja, a condição procurada é: a diferença simétrica entre B e C deve estar contida em A, mesmo que $B \neq C$.)

   ($\rightarrow$) Suponha que $A \cup B = A \cup C$. Seja x um elemento arbitrário de $(B - C) \cup (C - B)$. Caso 1: $x \in B - C$, ou seja $x \in B$ e $x \notin C$. Como $x \in B$ e $A \cup B = A \cup C$, segue-se que $x \in A \cup C$. Desta e de $x \notin C$, conclui-se que $x \in A$. Caso 2: análogo. Portanto, se $x \in (B - C) \cup (C - B)$, então $x \in A$. Logo, $(B - C) \cup (C - B) \subseteq A$.

   ($\rightarrow$) Suponha que $(B-C)\cup(C-B) \subseteq A$. Para provar, primeiramente, que $A\cup B \subseteq A\cup C$, seja $x \in A \cup B$. Caso 1: $x \in A$. Então $x \in A \cup C$. Caso 2: $x \in B$. Neste caso, se $x \in C$, $x \in A \cup C$, e se $x \notin C$, $x \in B - C$; e como $B - C \subseteq A$, $x \in A$ e, portanto, $x \in A \cup C$. Assim, se $x \in A \cup B$, então $x \in A \cup C$, ou seja $A \cup B \subseteq A \cup C$. De forma análoga, $A \cup C \subseteq A \cup B$. Portanto, $A \cup C = A \cup B$.

4. a) Basta provar que $\forall x[x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B}]$. Seja, então, um elemento x arbitrário. Tem-se:

$$
\begin{aligned}
x \in \overline{A \cup B} &\leftrightarrow x \notin A \cup B && \text{pela definição de complemento}\\
&\leftrightarrow \neg(x \in A \text{ ou } x \in B) && \text{pela definição de união}\\
&\leftrightarrow x \notin A \text{ e } x \notin B && \text{por DeMorgan}\\
&\leftrightarrow x \in \overline{A} \text{ e } x \in \overline{B} && \text{pela definição de complemento}\\
&\leftrightarrow x \in \overline{A} \cap \overline{B} && \text{pela definição de interseção.}
\end{aligned}
$$

b) Suponha que $A \cap B = A \cup B$. Inicialmente, prova-se que $A \subseteq B$. Seja x um elemento arbitrário de A. Neste caso, $x \in A \cup B$; e como $A \cap B = A \cup B$, $x \in A \cap B$. Logo, $x \in B$ e, portanto, $A \subseteq B$. Prova-se que $B \subseteq A$ de forma similar. Portanto, $A = B$. Conclui-se que se $A \cap B = A \cup B$ então $A = B$.

c) Basta provar que $\forall x[x \in (A-B) \cup (B-A) \leftrightarrow x \in (A \cup B) - (A \cap B)]$. Assim, seja um elemento x arbitrário. Tem-se:
($\rightarrow$) Suponha que $x \in (A-B) \cup (B-A)$. Caso 1: $x \in A - B$. Então $x \in A$ e $x \notin B$. Como $x \in A$, $x \in A \cup B$, e como $x \notin B$, $x \notin A \cap B$. Portanto, $x \in (A \cup B) - (A \cap B)$. O caso 2, $x \in B - A$, é similar.
($\rightarrow$) Suponha que $x \in (A \cup B) - (A \cap B)$. Então $x \in A \cup B$ e $x \notin A \cap B$. Segue-se, então, que $x \in A$ ou $x \in B$ e também que $x \notin A$ ou $x \notin B$. Assim, só se pode ter dois casos: o caso em que $x \in A$ e $x \notin B$ e caso em que $x \in B$ e $x \notin A$. Em outras palavras, $x \in A - B$ ou $x \in B - A$. Portanto, $x \in (A-B) \cup (B-A)$.

d) Basta provar que $\forall x[x \in A - (A-B) \leftrightarrow x \in A \cap B]$. Seja, então, um elemento x arbitrário. Tem-se:

$$\begin{aligned}
x \in A - (A-B) &\leftrightarrow x \in A \text{ e } x \notin A - B && \text{pela def. de diferença}\\
&\leftrightarrow x \in A \text{ e } (x \notin A \text{ ou } x \in B) && \text{pela def. de diferença}\\
&\leftrightarrow (x \in A \text{ e } x \notin A) \text{ ou } (x \in A \text{ e } x \in B) && \text{pela distrib. e/ou}\\
&\leftrightarrow x \in A \text{ e } x \in B\\
&\leftrightarrow x \in A \cap B && \text{pela def. de interseção.}
\end{aligned}$$

e) Basta provar que $\forall x[x \in (A-B) - C \leftrightarrow x \in A - (B \cup C]$. Assim, seja um elemento x arbitrário. Tem-se:

$$\begin{aligned}
x \in (A-B) - C &\leftrightarrow x \in A - B \text{ e } x \notin C && \text{pela def. de diferença}\\
&\leftrightarrow x \in A \text{ e } x \notin B \text{ e } x \notin C && \text{pela def. de diferença}\\
&\leftrightarrow x \in A \text{ e } \neg(x \in B \text{ ou } x \in C) && \text{pela lei de De Morgan}\\
&\leftrightarrow x \in A \text{ e } x \notin B \cup C && \text{pela def. de união}\\
&\leftrightarrow x \in A - (B \cup C) && \text{pela def. de diferença.}
\end{aligned}$$

f) Basta provar que $\forall x[x \in (A-B) - C \leftrightarrow x \in (A-C) - (B-C]$. Assim, seja um elemento x arbitrário. Tem-se:

$$\begin{aligned}
x \in (A-B) - (B-C) &\leftrightarrow (x \in A \text{ e } x \notin C) \text{ e } x \notin B - C\\
&\qquad\qquad \text{pela def. de diferença}\\
&\leftrightarrow (x \in A \text{ e } x \notin C) \text{ e } (x \notin B \text{ ou } x \in C)\\
&\qquad\qquad \text{pela def. de diferença}\\
&\leftrightarrow (x \in A \text{ e } x \notin C \text{ e } x \notin B) \text{ ou } (x \in A \text{ e } x \notin C \text{ e } x \in C)\\
&\qquad\qquad \text{pela distr. e/ou}\\
&\leftrightarrow x \in A \text{ e } x \notin C \text{ e } x \notin B\\
&\leftrightarrow x \in A - B \text{ e } x \notin C && \text{pela def. de diferença}\\
&\leftrightarrow x \in (A-B) - C && \text{pela def. de diferença}
\end{aligned}$$

g) Seja um par (x, y) arbitrário. Tem-se:

$$\begin{aligned}
(x,y) \in A \times (B \cap C) &\leftrightarrow x \in A \land y \in B \cap C && \text{pela def. de produto}\\
&\leftrightarrow x \in A \land y \in B \land y \in C && \text{pela def. de interseção}\\
&\leftrightarrow (x \in A \land y \in B) \land (x \in A \land y \in C)\\
&\leftrightarrow x \in A \times B \land x \in A \times C && \text{pela def. de produto}\\
&\leftrightarrow x \in (A \times B) \cap (A \times C) && \text{pela def. de interseção}
\end{aligned}$$

h) Seja um par (x, y) arbitrário. Tem-se:

$$\begin{aligned}
(x,y) \in (A \cap B) \times (C \cap D) &\leftrightarrow x \in (A \cap B) \wedge y \in (C \cap D) \\
&\qquad \text{pela def. de produto} \\
&\leftrightarrow x \in A \wedge x \in B \wedge y \in C \wedge y \in D \\
&\qquad \text{pela def. de interseção} \\
&\leftrightarrow (x \in A \wedge y \in C) \wedge (x \in B \wedge y \in D) \\
&\qquad \text{por associatividade} \\
&\leftrightarrow x \in A \times C \wedge x \in B \times D \\
&\qquad \text{pela def. de produto} \\
&\leftrightarrow x \in (A \times C) \cap (B \times D) \\
&\qquad \text{pela def. de interseção}
\end{aligned}$$

5. As partições de $\{1,2\}$ são: $\{\{1\},\{2\}\}$ e $\{\{1,2\}\}$. As partições de $\{1,2,3\}$ são: $\{\{1\},\{2\},\{3\}\}$, $\{\{1\},\{2,3\}\}$, $\{\{2\},\{1,3\}\}$, $\{3\},\{1,2\}\}$ e $\{\{1,2,3\}\}$. E as partições de $\{1,2,3,4\}$ são: $\{\{1\},\{2\},\{3\},\{4\}\}$, $\{\{1\},\{2\},\{3,4\}\}$, $\{\{1\},\{3\},\{2,4\}\}$, $\{\{1\},\{4\},\{2,3\}\}$, $\{\{2\},\{3\},\{1,4\}$, $\{\{2\},\{4\},\{1,3\}\}$, $\{\{3\},\{4\},\{1,2\}\}$, $\{\{1\},\{2,3,4\}\}$, $\{\{2\},\{1,3,4\}\}$, $\{\{3\},\{1,2,4\}\}$, $\{\{4\},\{1,2,3\}\}$, $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$ e $\{\{1,2,3,4\}\}$.

   Segue a função *part*(A), que retorna o conjunto das partições do conjunto (finito) A:

   Entrada: um conjunto finito A.
   Saída: o conjunto das partições de A.
   se $A = \emptyset$ **então** retorne $\emptyset$ **fimse**;
   $R \leftarrow \emptyset$;
   selecione um elemento $a \in A$;
   para cada $B \subset A$ tal que $a \in B$ **faça**
       para cada $X \in part(A - B)$ **faça**
           $R \leftarrow R \cup \{\{B\} \cup X\}$;
       fimpara
   fimpara;
   retorne $R \cup \{\{A\}\}$.

1.4 Relações

1. a) A relação $\subset$ é transitiva, não é reflexiva nem simétrica.
   b) A relação não é reflexiva, nem simétrica nem transitiva.
   c) A relação é reflexiva e transitiva, e não é simétrica.
   d) A relação é reflexiva e transitiva, e não é simétrica.
   e) A relação é reflexiva, simétrica e transitiva.

2. Sejam $R_1 \subseteq A^2$ e $R_2 \subseteq B^2$

   a) Se R_1 e R_2 são reflexivas, $R_1 \cup R_2$ é reflexiva sobre $A \cup B$: Seja $x \in A \cup B$. Se $x \in A$, $(x,x) \in R_1$, pois R_1 é reflexiva, e se $x \in B$, $(x,x) \in R_2$, pois R_2 é reflexiva. Assim, $(x,x) \in R_1 \cup R_2$.

Se R_1 e R_2 são reflexivas, $R_1 \cap R_2$ é reflexiva sobre $A \cap B$: Seja $x \in A \cap B$. Como $x \in A$ e $x \in B$, $(x, x) \in R_1$ e $(x, x) \in R_2$ pois R_1 e R_2 são reflexivas. Assim, $(x, x) \in R_1 \cap R_2$.

b) Se R_1 e R_2 são simétricas, $R_1 \cup R_2$ é simétrica sobre $A \cup B$: Sejam $x, y \in A \cup B$. Se $x, y \in A$ e $(x, y) \in R_1$, então $(y, x) \in R_1$ e, analogamente, se $x, y \in B$ e $(x, y) \in R_2$, então $(y, x) \in R_2$, pois R_1 e R_2 são simétricas. Por outro lado, se $x \in A - B$ e $y \in B - A$, ou vice-versa, ou seja, x e y não pertencem ao mesmo conjunto, não se pode ter $(x, y) \in R_1$ nem $(x, y) \in R_2$. Assim, em qualquer caso, se $x, y \in A \cup B$ e $(x, y) \in R_1 \cup R_2$, $(y, x) \in R_1 \cup R_2$.

Se R_1 e R_2 são simétricas, $R_1 \cap R_2$ é simétrica sobre $A \cap B$: Sejam $x, y \in A \cap B$. Como $x, y \in A$ e $x, y \in B$ $(y, x) \in R_1$ e $(y, x) \in R_2$, pois R_1 e R_2 são simétricas. Portanto, se $x, y \in A \cap B$ e $(x, y) \in R_1 \cap R_2$, $(y, x) \in R_1 \cap R_2$.

c) Se R_1 e R_2 são transitivas, $R_1 \cup R_2$ pode não ser transitiva. Por exemplo, $R_1 = \{(a, b)\}$ sobre $\{a, b\}$ e $R_2 = \{(b, c)\}$ sobre $\{b, c\}$; tem-se que $R_1 \cup R_2 = \{(a, b), (b, c)\}$ sobre $\{a, b, c\}$, que não é transitiva, pois $(a, c) \notin R_1 \cup R_2$.

A relação $R_1 \cap R_2$ é transitiva sobre $A \cap B$: Dado que $(x, y) \in R_1 \cap R_2$ e $(y, z) \in R_1 \cap R_2$, segue-se que $(x, y) \in R_1$ e $(y, z) \in R_1$, e também que $(x, y) \in R_2$ e $(y, z) \in R_2$. Como R_1 e R_2 são transitivas, deduz-se que $(x, z) \in R_1$ e $(x, z) \in R_2$. Logo, $(x, z) \in R_1 \cap R_2$.

3. $(\rightarrow)$ Suponha que R é simétrica. Sejam x e y elementos arbitrários tais que $(x, y) \in R$. Como R é simétrica, segue-se que $(y, x) \in R$. Desta última, segue-se que $(x, y) \in R^{-1}$. Logo, se $(x, y) \in R$, então $(x, y) \in R^{-1}$, ou seja, $R \subseteq R^{-1}$. De forma similar, mostra-se que $R^{-1} \subseteq R$. Portanto, $R = R^{-1}$.

   $(\leftarrow)$ Suponha que $R = R^{-1}$ e seja $(x, y) \in R$. Segue-se que $(x, y) \in R^{-1}$ e, portanto, $(y, x) \in R$. Logo, se $(x, y) \in R$ então $(y, x) \in R$. Como (x, y) é um elemento arbitrário de R, conclui-se que R é simétrica.

4. $(\rightarrow)$ Suponha que R é reflexiva sobre um conjunto A. Seja x um elemento arbitrário de A. Como R é reflexiva, segue-se que $(x, x) \in R$. Segue-se, pela definição de inversa, que $(x, x) \in R^{-1}$. Logo, R^{-1} é reflexiva sobre A.

   $(\leftarrow)$ Suponha que R^{-1} é reflexiva sobre um conjunto A. Seja x um elemento arbitrário de A. Como R^{-1} é reflexiva, segue-se que $(x, x) \in R^{-1}$. Segue-se, pela definição de inversa, que $(x, x) \in R$. Logo, R é reflexiva sobre A.

5. $(\rightarrow)$ Suponha que R é anti-simétrica. Sejam x e y elementos arbitrários de A tais que $(x, y) \in R \cap R^{-1}$, ou seja, $(x, y) \in R$ e $(x, y) \in R^{-1}$. Desta última, segue-se que $(y, x) \in R$. Como R é anti-simétrica, $(x, y) \in R$ e $(y, x) \in R$, segue-se que $x = y$ e, portanto, $(x, y) \in \iota_A$. Assim, $R \cap R^{-1} \subseteq \iota_A$.

   $(\leftarrow)$ Suponha que $R \cap R^{-1} \subseteq \iota_A$. Sejam x e y tais que $(x, y) \in R$ e $(y, x) \in R$. Como $(y, x) \in R$, $(x, y) \in R^{-1}$, e, portanto, $(x, y) \in R \cap R^{-1}$. Como $R \cap R^{-1} \subseteq \iota_A$, segue-se que $(x, y) \in \iota_A$ e, portanto, $x = y$. Conclui-se que se $(x, y) \in R$ e $(y, x) \in R$, então $x = y$. Portanto, R é anti-simétrica.

6. Nesta questão, considere que se o denominador nas operações de divisão for 0, o resultado é sempre o mesmo ("indefinido") e diferente de qualquer outro resultado.

   Como $x_1/x_2 = x_1/x_2$ para quaisquer $x_1, x_2 \in \mathbf{N}$, R é reflexiva. Suponha que $x_1/x_2 = y_1/y_2$, para $x_1, x_2, y_1, y_2 \in \mathbf{N}$. Segue-se que $y_1/y_2 = x_1/x_2$. Logo, R é simétrica. Supondo-se que $x_1/x_2 = y_1/y_2$ e $y_1/y_2 = z_1/z_2$, conclui-se que $x_1/x_2 = z_1/z_2$. Portanto, R é transitiva. Como R é reflexiva, simétrica e transitiva, R é uma relação de equivalência.

Para cada par $(x_1, x_2) \in \mathbf{N}^2$ há a classe de equivalência $\{(y_1, y_2) \in \mathbf{N}^2 \mid y_1/y_2 = x_1/x_2\}$, ou seja a cada número racional, r, corresponde a classe de equivalência constituída dos pares de naturais (x_1, x_2) tais que $r = x_1/x_2$.

7. a) Fecho reflexivo: $\{(a,a),(c,c),(d,d),(e,e)\} \cup R$.
   b) Fecho simétrico: $\{(a,d),(b,a)\} \cup R$.
   c) Fecho transitivo: $\{(c,a),(c,b),(c,c),(d,b),(d,d)\} \cup R$.
   d) Fecho reflexivo e simétrico: $\{(a,a),(c,c),(d,d),(e,e),(a,d),(b,a)\} \cup R$.
   e) Fecho reflexivo e transitivo: $\{(a,a),(c,c),(d,d),(e,e),(c,a),(c,b),(d,b)\} \cup R$.
   f) Fecho simétrico e transitivo: $\{(a,d),(b,a),(c,a),(c,b),(c,c),(d,b),(d,d)\} \cup R$.
   g) Fecho reflexivo, simétrico e transitivo:
   $\{(a,a),(c,c),(d,d),(e,e),(a,d),(b,a),(c,a),(c,b),(d,b)\} \cup R$.

1.5 Funções

1. O número máximo para $R \subseteq A \times B$ ser uma função é $|R| = |A|$, já que não se pode ter $(x,y) \in f$ e $(x,z) \in f$ se $y \neq z$.

2. Sejam $f : A \to B$, $g : C \to D$ e $h = f \cup g$. Então:

$$h : A \cup C \to B \cup D \text{ se, e somente se, } \forall x \in A \cap C f(x) = g(x).$$

   Prova:

   $(\to)$ Suponha que $h : A \cup C \to B \cup D$. Seja um elemento arbitrário x de $A \cap C$. Como $h = f \cup g$ e $h : A \cup C \to B \cup D$, segue-se que $h(x) = f(x) = g(x)$.

   $(\leftarrow)$ Suponha que $\forall x \in A \cap C f(x) = g(x)$. Seja y um elemento arbitrário de $A \cup C$. Para mostrar existe um único $z \in B \cup D$ tal que $(y,z) \in h$, serão considerados 3 casos:
   Caso 1: $y \in A - C$. Como $f : A \to B$, $h = f \cup g$ e $y \in A$, um z tal que $(y,z) \in h$ é $z = f(y)$. E como $g : C \to D$, $h = f \cup g$ e $y \notin C$, tal z é único.
   Caso 2: $y \in C - A$. Como $g : C \to D$, $h = f \cup g$ e $y \in C$, um z tal que $(y,z) \in h$ é $z = g(y)$. E como $f : A \to B$, $h = f \cup g$ e $y \notin A$, tal z é único.
   Caso 3: $y \in A \cap C$. Como $f : A \to B$, $g : C \to D$, $h = f \cup g$ e $\forall x \in A \cap C f(x) = g(x)$, o único z tal que $(y,z) \in h$ é $z = f(y) = g(y)$.

3. a) f não é injetora, pois $f(0) = f(1) = 0$. É sobrejetora, pois $f(2n) = n$ para todo $n \in \mathbf{N}$.
   b) g é injetora, pois se $g(n) = g(k)$, então $k = n$. Ela não é sobrejetora, pois não existe $n \in \mathbf{N}$ tal que $g(n) = 2$: $g(1) = 1$ e $g(2) = 3$ e g é crescente.
   c) h é injetora: Suponha que $h(n) = h(k)$. Se n e k forem ambos pares ou ambos ímpares, para que $n - 1 = k - 1$ ou $n + 1 = k + 1$, deve-se ter que $n = k$. Por outro lado se um é par e o outro é ímpar, para que $n + 1 = k - 1$, deve-se ter que $n + 2 = k$; mas, para que isto seja verdade, n e k não podem ser um par e o outro ímpar!

      h é sobrejetora, pois $h(n+1) = n$ para todo número n par a partir de 0, e $h(n-1) = n$ para todo número n ímpar a partir de 1.

      Portanto, h é bijetora. Da última sentença acima, vê-se que a $h^{-1} = h$.

4. Sejam $|A| = n$ e $|B| = k$.

a) Para cada $a \in A$, $f(a)$ pode ser qualquer elemento de B. Assim, existem k^n funções totais possíveis.

b) Para cada $a \in A$, $f(a)$ pode ser indefinido ou qualquer elemento de B. Assim, existem $(k+1)^n$ funções parciais possíveis.

c) Se $n > k$, não há função injetora. Suponha que $n \leq k$. Escolhido um elemento de B para ser $f(a)$, ele não pode mais ser $f(b)$ para $b \neq a$. Assim, existem $P(k,n) = k.(k-1)\ldots(k-n+1) = k!/(k-n)!$ funções injetoras possíveis, se $n \leq k$.

d) Se $n < k$, não há função sobretora. Suponha que $n \geq k$. Deve ser escolhido um elemento de eA tal que $f(a)$ seja um elemento de B, para cada elemento de B. Para isto existem $P(n,k) = n.(n-1)\ldots(n-k+1) = n!/(n-k)!$ possibilidades. Para cada uma delas, os $n-k$ elementos restantes de A podem, cada um deles, ser mapeado para qualquer um dos elementos de B: são k^{n-k} possibilidades. Assim, existem $(n!.k^{n-k})/(n-k)!$ funções sobrejetoras possíveis, se $n \geq k$.

e) Quando $n = k$, existe uma única função bijetora. Se $n \neq k$, não existe função bijetora.

5. a) Sejam x e y elementos arbitrários de A tais que $x \neq y$. Como f é injetora, $f(x) \neq f(y)$. E como g é injetora, $g(f(x)) \neq g(f(y))$. Portanto, se $x \neq y$, então $g(f(x)) \neq g(f(y))$. Conclui-se que $g \circ f$ é injetora.

   b) Seja $y \in C$ arbitrário. Como g é sobrejetora, existe $z \in B$ tal que $g(z) = y$. E como f é sobrejetora, existe $x \in A$ tal que $f(x) = z$, ou ainda, $g(f(x)) = y$. Logo, para todo $y \in C$ existe $x \in A$ tal que $g(f(x)) = y$. Portanto, $g \circ f$ é sobrejetora.

   c) Dos dois resultados acima segue-se que $g \circ f$ é bijetora.

6. Seja $f : A \to B$. Seja $C = \{b \in B \,|\, f(a) = b$ para algum $a \in A\}$. Seja a função sobrejetora $g : A \to C$ tal que $g(a) = f(a)$ para todo $a \in A$. Seja a função injetora $h : C \to B$ tal que $h(c) = c$ para todo $c \in C$. Então $f = h \circ g$.

7. Como $g \circ f = f \circ g$, $g(f(n)) = f(g(n))$ para todo $n \in \mathbf{R}$. Logo, $c(an+b)+d = a(cn+d)+b$, ou seja, $acn + bc + d = acn + ad + b$, ou ainda, $bc + d = ad + b$. Tem-se, então, que $b(c-1) = d(a-1)$.

1.6 Conjuntos Enumeráveis

1. a) O conjunto $X = \{n \in \mathbf{N} \,|\, n \, mod \, 10 = 0\}$ é enumerável, pois é um subconjunto de $\mathbf{N}$. Uma função bijetora seria $g : \mathbf{N} \to X$, tal que $g(n) = 10n$.

   b) O conjunto $\mathbf{N}^3 = \{(n_1, n_2, n_3) \,|\, n_1, n_2, n_3 \in \mathbf{N}\}$ é enumerável. Uma função bijetora seria $h : \mathbf{N}^3 \to \mathbf{N}$, tal que $h(n_1, n_2, n_3) = f(f(n_1, n_2), n_3)$, onde $f : \mathbf{N}^2 \to \mathbf{N}$ é tal que $f(i,j) = (i+j)(i+j+1)/2 + i$.

   c) O conjunto $W = \{n \in \mathbf{R} \,|\, 0 < n < 1\}$ não é enumerável, como será mostrado por contradição. Suponha que W é enumerável. Seja, então, r_0, r_1, r_2, $\ldots$ uma enumeração dos elementos de W. Será denotado por $d_i(r)$ o i-ésimo dígito após a vírgula da expansão decimal do número r de W. Por exemplo, $d_1(0,53) = 5$, $d_7(0,53) = 0$. Seja o número k entre 0 e 1 tal que $d_i(k) = d_i(r_i) + 5 \, mod \, 10$ para $i \in \mathbf{N}$. Tal número difere de qualquer r_i no i-ésimo dígito após a vírgula. Logo $k \neq r_i$ para $i \in \mathbf{N}$. Contradição; W não é enumerável.

2. Suponha que tal conjunto seja enumerável. Então existe uma enumeração $f_0, f_1, f_2, \ldots$ de todas as funções de $\mathbf{N}$ para $\{0,1\}$. Seja a função $g\colon \mathbf{N} \to \{0,1\}$ tal que $g(n) = 1 - f_n(n)$. Ora, $g(n) \neq f_n(n)$ para todo $n \in \mathbf{N}$, e, portanto, $g \neq f_n$ para todo $n \in \mathbf{N}$. Logo, a suposição da enumerabilidade das funções não se sustenta.

3. Suponha que tal conjunto seja enumerável. Então existe uma enumeração $f_0, f_1, f_2, \ldots$ de todas as funções de $\mathbf{N}$ para $\mathbf{N}$ monotônicas crescentes. Seja a função $h\colon \mathbf{N} \to \mathbf{N}$ tal que $h(n) = 1 + \sum_{k=0}^{n} f_k(k)$. Veja que, como as funções f_k são monotônicas crescentes, então $f_k(k) > 0$ para $k > 0$. Assim, h, além de diferente de f_n para todo $n \in \mathbf{N}$. é monotônica crescente. Logo, a suposição da enumerabilidade das funções monotônicas crescentes é incorreta.

4. Seja um conjunto enumerável arbitrário A e suponha que $B \subseteq A$. Se B é finito, é contável, por definição. Suponha que B é infinito. Será mostrado que B é enumerável construindo-se uma função bijetora $g : \mathbf{N} \to B$. Como A é enumerável, existe uma função bijetora $f : \mathbf{N} \to A$; assim sendo, pode-se dizer que $A = \{f(k) \,|\, k \in \mathbf{N}\}$. A função g pode ser construída da seguinte forma:

   - $g(0) = f(m)$, onde m é o *menor* número natural tal que $f(k) \in B$;
   - para $i > 0$, $g(i) = f(k)$, onde k é o *menor* número natural tal que $f(k) \in B$ e $k > j$, sendo j tal que $g(i-1) = f(j)$.

5. Como todo subconjunto de conjunto enumerável é contável (questão 4), sabe-se que $A - B$ é contável. Como $(A - B) \cup B = A \cup B$, basta mostrar que $(A - B) \cup B$ é contável, sendo que $(A - B) \cap B = \emptyset$. No caso em ambos $A - B$ e B são finitos, $(A - B) \cup B$ é finito e, portanto, contável. No caso em que um deles é finito e o outro não, seja $\{a_0, a_1, \ldots, a_m\}$ o conjunto finito e suponha que existe uma função bijetora f de $\mathbf{N}$ para o conjunto infinito. Então, pode-se construir uma função bijetora $h : \mathbf{N} \to A \cup B$, onde $h(k) = a_k$ para $0 \leq k \leq m$ e $h(k) = f(k - m - 1)$ para $k \geq m + 1$. Agora, se ambos $A - B$ e B são infinitos, sejam $f : \mathbf{N} \to A - B$ e $g : \mathbf{N} \to B$ bijetoras. Então pode-se construir uma função bijetora $h : \mathbf{N} \to A \cup B$, onde $h(2k) = f(k)$ e $h(2k - 1) = g(k)$ para $k \in \mathbf{N}$.

   A interseção é subconjunto dos dois conjuntos. Logo é contável (questão 4).

   O produto de conjuntos finitos é finito. Se um dos conjuntos é finito e o outro não, seja $\{a_0, a_1, \ldots, a_m\}$ o conjunto finito e suponha que existe uma função bijetora f de $\mathbf{N}$ para o conjunto infinito. Sem perda de generalidade, seja A o conjunto finito. Então, pode-se construir uma função bijetora $h : A \times B \to \mathbf{N}$, onde $h(i, j) = j(m + 1) + i$ para $0 \leq i \leq m$ e $j \in \mathbf{N}$. Se os dois conjuntos forem infinitos, sejam $f : A \to \mathbf{N}$ e $g : B \to \mathbf{N}$ bijetoras. A função $h : A \times B \to \mathbf{N}$, onde $h(f(a), g(b)) = (f(a) + g(b))(f(a) + g(b) + 1)/2 + f(a)$ é bijetora.

6. Seja $|F| = n$. A cardinalidade do conjunto das funções totais $f : F \to E$ é igual à do conjunto E^n: existe uma função bijetora que, a cada função f faz corresponder a n-upla $(f(a_1), f(a_2), \ldots, f(a_n))$, onde a_1, a_2, $\ldots$, a_n são os elementos de F. Como E^n é enumerável, segue-se que o conjunto em questão é enumerável.

1.7 Definições Recursivas

1. Definição recursiva de $f : \mathbf{N} \to \mathbf{N}$, tal que $f(n) = \sum_{k=1}^{n} k$:

   a) $f(1) = 1$;

b) $f(n) = f(n-1) + n$ para $n > 1$.

2. Seja um universo U. O número de elementos do conjunto potência de um conjunto finito de elementos de U , pode ser definido recursivamente assim:

   a) $|\mathcal{P}(\emptyset)| = 1$;
   b) $|\mathcal{P}(X \cup \{a\})| = 2|\mathcal{P}(X)|$ para todo $a \in U$.

3. Definição recursiva da representação de números binários sem zeros à esquerda, $r : \mathbf{N} \to B$, onde B é o conjunto das seqüências de dígitos binários:

   a) $r(0) = 0$, $r(1) = 1$;
   b) $r(n) = r(\lfloor n/2 \rfloor)(n \ mod\ 2)$ para $n > 1$.

   Assim, por exemplo, $r(5) = r(2)1 = r(1)01 = 101$.

4. Definição recursiva da seqüência de Fibonacci:

   a) $a_0 = 0$ e $a_1 = 1$;
   b) $a_n = a_{n-2} + a_{n-1}$ para $n \geq 2$.

5. Definição recursiva de multiplicação sobre $\mathbf{N}$:

   a) $m \times 0 = 0$ para todo $m \in \mathbf{N}$;
   b) $m \times s(n) = m + (m \times n)$ para $m, n \in \mathbf{N}$.

6. Definição recursiva de LP$'$, semelhante a LP, porém com omissão e/ou excesso de parênteses:

   a) cada variável proposicional pertence a LP$'$;
   b) se $\alpha, \beta \in$ LP$'$, então pertencem a LP$'$: $\neg\alpha$, $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \to \beta$, $\alpha \leftrightarrow \beta$ e (α).

1.8 Indução Matemática

1. Só existe um conjunto de 0 elementos: $\emptyset$; e $2^0 = 1 = |\{\emptyset\}| = |\mathcal{P}(\emptyset)|$. Seja $n \geq 0$. Suponha, como hipótese de indução, que $|\mathcal{P}(A)| = 2^n$ para conjuntos A de n elementos. Seja um conjunto B de $n+1$ elementos e a um de seus elementos. Tem-se: $\mathcal{P}(B) = \mathcal{P}(B - \{a\}) \cup \{X \cup \{a\} \,|\, X \in \mathcal{P}(B - \{a\})\}$. Pela hipótese de indução, $|\mathcal{P}(B - \{a\})| = 2^n$, e como $\mathcal{P}(B - \{a\})$ e $\{X \cup \{a\} \,|\, X \in \mathcal{P}(B - \{a\})\}$ têm o mesmo número de elementos, $|\mathcal{P}(B)| = 2^n + 2^n = 2^{n+1}$.

2. a) $\sum_{k=0}^{0} k^2 = 0^2 = 0 = 0(0+1)(2 \times 0 + 1)/6$. Seja n um número natural arbitrário. Suponha, como hipótese de indução, que $\sum_{k=0}^{n} k^2 = n(n+1)(2n+1)/6$. Basta provar, então, que $\sum_{k=0}^{n+1} k^2 = (n+1)(n+2)(2n+3)/6$. De fato:

   $$\begin{aligned}\textstyle\sum_{k=0}^{n+1} k^2 &= [\textstyle\sum_{k=0}^{n} k^2] + (n+1)^2 \\ &= [n(n+1)(2n+1)/6] + (n+1)^2 \quad \text{pela hipótese de indução} \\ &= [n(n+1)(2n+1) + 6(n+1)^2]/6 \\ &= (n+1)[n(2n+1) + 6(n+1)]/6 \\ &= (n+1)(2n^2 + 7n + 6)/6 \\ &= (n+1)(n+2)(2n+3)/6.\end{aligned}$$

   b) $\sum_{k=0}^{0} k^3 = 0^3 = 0 = 0^2 = [0(0+1)/2]^2$. Seja $n \geq 0$ arbitrário. Suponha, como hipótese de indução, que $\sum_{k=0}^{n} k^3 = [n(n+1)/2]^2$. Basta provar, então, que $\sum_{k=0}^{n+1} k^3 = [(n+1)(n+2)/2]^2$. De fato:

$$
\begin{aligned}
\textstyle\sum_{k=0}^{n+1} k^3 &= [\textstyle\sum_{k=0}^{n} k^3] + (n+1)^3 \\
&= [n(n+1)/2]^2 + (n+1)^3 \qquad \text{pela hipótese de indução} \\
&= [n^2(n+1)^2 + 4(n+1)^3]/4 \\
&= [(n+1)^2(n^2+4n+4)]/4 \\
&= [(n+1)^2(n+2)^2]/4 \\
&= [(n+1)(n+2)/2]^2.
\end{aligned}
$$

c) Inicialmente, obsereve que: $2^{2\times 0} - 1 = 2^0 - 1 = 1 - 1 = 0$, que é divisível por 3. Seja $n \geq 0$. Suponha, como hipótese de indução, que $2^{2n} - 1$ é divisível por 3. Então: $2^{2(n+1)} - 1 = 2^{2n+2} - 1 = 2^{2n} \times 2^2 - 1 = 4 \times 2^{2n} - 1 = 3 \times 2^{2n} + 2^{2n} - 1$. Como 3×2^{2n} é divisível por 3 e, pela hipótese de indução, $2^{2n} - 1$ também é divisível por 3, segue-se que $2^{2(n+1)} - 1$ é divisível por 3.

d) $0^3 - 0 = 0$, que é divisível por 6. Seja $n \geq 0$. Hipótese de indução: $n^3 - n$ é divisível por 6. Deve-se provar que $(n+1)^3 - (n+1)$ é divisível por 6. Tem-se: $(n+1)^3-(n+1) = n^3+3n^2+3n+1-n-1 = (n^3-n)+(3n^2+3n) = (n^3-n)+3n(n+1)$. Como $n(n+1)$ é sempre um número par, $3n(n+1)$ é divisível por 6. E como, pela hipótese de indução, $n^3 - n$ também é divisível por 6, segue-se que $(n+1)^3 - (n+1)$ é divisível por 6.

e) $7^0 - 1 = 1 - 1 = 0$, que é divisível por 6. Seja $n \geq 0$. Suponha, como hipótese de indução, que $7^n - 1$ é divisível por 6. Tem-se: $7^{n+1} - 1 = 7^n - 1 + 6 \times 7^n$. Como 6×7^n é divisível por 6 e, pela hipótese de indução, $7^n - 1$ é divisível por 6, conclui-se que $7^{n+1} - 1$ é divisível por 6.

3. a) Tem-se: $\sum_{k=1}^{1}[k(k+1)] = 1(1+1) = 2 = 1(2)(3)/3 = 1(1+1)(1+2)/3$. Seja $n \geq 1$. Suponha, como hipótese de indução, que $\sum_{k=1}^{n}[k(k+1)] = n(n+1)(n+2)/3$. Basta, então, provar que $\sum_{k=1}^{n+1}[k(k+1)] = (n+1)(n+2)(n+3)/3$. De fato:

$$
\begin{aligned}
\textstyle\sum_{k=1}^{n+1}[k(k+1)] &= [\textstyle\sum_{k=1}^{n} k(k+1)] + (n+1)(n+2) \\
&= [n(n+1)(n+2)/3] + (n+1)(n+2) \qquad \text{pela hipótese de indução} \\
&= [n(n+1)(n+2) + 3(n+1)(n+2)]/3 \\
&= (n+1)(n+2)(n+3)/3.
\end{aligned}
$$

b) $\sum_{k=1}^{1} 2^k = 2^1 = 2 = 2\times 1 = 2(2-1) = 2(2^1-1)$. Seja $n \geq 1$. Suponha, como hipótese de indução, que $\sum_{k=1}^{n} 2^k = 2(2^n - 1)$. Tem-se: $\sum_{k=1}^{n+1} 2^k = [\sum_{k=1}^{n} 2^k] + 2^{n+1} = 2(2^n - 1) + 2^{n+1}$, pela hipótese de indução. Logo, $\sum_{k=1}^{n+1} 2^k = 2^{n+1} - 2 + 2^{n+1} = 2(2^{n+1} - 1)$, como requerido.

c) Inicialmente, veja que $\sum_{k=1}^{1}[1/k(k+1)] = 1/(1+1)$. Seja $n \geq 1$ arbitrário, e suponha, como hipótese de indução, que $\sum_{k=1}^{n}[1/k(k+1)] = n/(n+1)$. Então:

$$
\begin{aligned}
\textstyle\sum_{k=1}^{n+1}[1/k(k+1)] &= [\textstyle\sum_{k=1}^{n}[1/k(k+1)]] + 1/(n+1)(n+2) \\
&= [n/(n+1)] + 1/(n+1)(n+2) \qquad \text{pela hipótese de indução} \\
&= [n(n+2)+1]/[(n+1)(n+2)] \\
&= [n^2+2n+1]/[(n+1)(n+2)] \\
&= (n+1)^2/[(n+1)(n+2)] \\
&= (n+1)/(n+2).
\end{aligned}
$$

Logo, pelo princípio de indução, $\sum_{k=1}^{n}[1/k(k+1)] = n/(n+1)$ para todo $n \geq 1$.

d) $1^3+(1+1)^3+(1+2)^3 = 1+8+27 = 36$, que é divisível por 9. Seja um número natural n arbitrário maior ou igual a 1. Suponha, como hipótese de indução, que $n^3+(n+1)^3+(n+2)^3$ é divisível por 9. Deve-se mostrar que $(n+1)^3+(n+2)^3+(n+3)^3$ é divisível por 9. Tem-se que $(n+1)^3+(n+2)^3+(n+3)^3 = (n+1)^3+(n+2)^3+n^3+9n^2+27n+27$, ou seja, $(n+1)^3 + (n+2)^3 + (n+3)^3 = n^3 + (n+1)^3 + (n+2)^3 + 9(n^2+3n+3)$. Deduz-se, então, aplicando-se a hipótese de indução, que $(n+1)^3+(n+2)^3+(n+3)^3$ é divisível por 9.

4. Seja n um número natural arbitrário. Suponha, como hipótese, que

$$F(k) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right]$$

para $k < n$. Serão considerados 3 casos:

Caso 1: $n = 0$. Neste caso, $F(0) = 0$ por definição, e $(1/\sqrt{5})[((1+\sqrt{5})/2)^0 - ((1-\sqrt{5})/2)^0] = 1 - 1 = 0$.

Caso 2: $n = 1$. Neste caso, $F(1) = 1$ por definição, e $(1/\sqrt{5})[((1+\sqrt{5})/2)^1 - ((1-\sqrt{5})/2)^1] = (1+\sqrt{5}-1+\sqrt{5})/(2\sqrt{5}) = 1$.

Caso 3: $n \geq 2$. Neste caso, $F(n) = F(n-1) + F(n-2)$ por definição. Aplicando-se a hipótese de indução, obtém-se:

$$F(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\right].$$

Assim,

$$F(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}+1\right)\right].$$

Verifica-se facilmente que:

$$\frac{1+\sqrt{5}}{2}+1 = \left(\frac{1+\sqrt{5}}{2}\right)^2 \text{ e } \frac{1-\sqrt{5}}{2}+1 = \left(\frac{1-\sqrt{5}}{2}\right)^2.$$

Portanto,

$$F(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

5. Será usada indução forte sobre o número de conectivos. Assim, seja $n \geq 0$, e suponha que o resultado valha para sentenças com menos de n conectivos. Deve-se provar, então, que o resultado vale para sentenças com n conectivos. Considera-se dois casos:

   (a) $n = 0$. Uma sentença sem conectivos é uma variável proposicional, e esta tem apenas dois prefixos: λ e ela mesma. Em ambos o número de abre e fecha parênteses é zero.

   (b) $n > 0$. Uma sentença com conectivos é da forma $\neg\alpha$ ou $(\alpha \oplus \beta)$, onde $\oplus \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$:

   i) $\neg\alpha$. Como α tem $n-1$ conectivos, o resultado vale para α, pela hipótese de indução. Segue-se que vale também para $\neg\alpha$, que não tem outros parênteses que os de α.

   ii) $(\alpha \oplus \beta)$. Como α e β têm menos de n conectivos, o resultado vale para ambos, pela hipótese de indução. Segue-se que o resultado vale também para $\alpha \oplus \beta$. E o resultado continua valendo ao se colocar os parênteses externos.

1.9 Grafos

1. Isto segue do fato de que a soma dos graus dos vértices é par: em um grafo sem arestas tal soma é zero, e cada aresta acrescenta 2 unidades à soma.

2. Será feita uma prova por indução sobre o número de vértices. A menor árvore, que é da forma $(\{v\}, \emptyset, v)$, tem um vértice e nenhuma aresta. Seja um número $n \geq 1$ e suponha, como hipótese de indução, que a proposição é verdadeira para árvores com n vértices. Uma árvore com $n + 1$ vértices é da forma $(V \cup \{v\}, A \cup \{\{v, v'\}\}, r)$, onde $v \in V$, $v' \notin V$ e (V, A, r) é uma árvore de n vértices. Pela hipótese de indução, $|A| = n - 1$, ou ainda, $|A| + 1 = (n + 1) - 1$, o que mostra que a proposição vale para árvores de $n + 1$ vértices, já que estas têm $|A| + 1$ arestas.

3. Isto segue do fato de que a cada aresta introduzida no grafo, a soma dos graus dos vértices aumenta de 2 unidades.

4. O número de arestas de K_n é $C(n, 2) = n(n + 1)/2$.

5. a) Uma árvore binária de altura 0 tem apenas 1 vértice e ele é folha; e $2^0 = 1$. Seja $n \geq 0$. Suponha, como hipótese de indução, que árvores binárias de altura n possuem, no máximo, 2^n folhas. Uma árvore binária B de altura $n + 1$ possue um máximo de folhas quando as duas subárvores da raiz possuem um máximo de folhas. Isto acontece quando ambas têm altura n. Assim, pela hipótese de indução, elas possuem 2^n folhas. Logo a árvore B tem $2^n + 2^n = 2^{n+1}$ folhas.

   b) Uma árvore binária de altura 0 tem apenas 1 vértice; e $2^{0+1} - 1 = 1$. Seja $n \geq 0$. Suponha, como hipótese de indução, que árvores binárias de altura n possuem, no máximo, $2^{n+1} - 1$ vértices. Uma árvore binária B de altura $n+1$ possue um máximo de vértices quando as duas subárvores da raiz possuem um máximo de vértices. Isto acontece quando ambas têm altura n. Assim, pela hipótese de indução, elas possuem $2^{n+1} - 1$ vértices. Logo a árvore B tem os $2^{n+1} - 1$ vértices de cada uma mais a raiz: $2^{n+1} - 1 + 2^{n+1} - 1 + 1 = 2 \times 2^{n+1} + 1 = 2^{n+2} + 1$.

6. Será usada a definição de árvore do livro.

   (a)→(b) Por indução sobre o número de vértices. Se a árvore tem 1 vértice não tem arestas. Logo, satisfaz (b). Seja $n \geq 1$, e suponha que (b) vale para árvores de n vértices. Seja uma árvore A de $n + 1$ vértices. Pela definição, tal árvore é formada de uma árvore de n vértices pela inclusão de um vértice *novo* e uma nova aresta. Como, pela hipótese de indução, (b) vale para árvore de n vértices, então continua valendo para A.

   (b)→(c) Sendo o grafo acíclico, se existir um caminho simples de um vértice a outro, ele é único. Assim, basta mostrar a existência de caminho simples. Isto será feito por indução sobre o número de vértices. Se o grafo tem 1 vértice, existe caminho simples dele até ele mesmo. Seja $n \geq 1$, e suponha que (c) vale para grafos (que satisfazem (b)) de n vértices ou menos. Seja Seja um grafo G de $n + 1$ vértices que satisfaça (b). Seja v um vértice arbitrário de G. Suponha que existam k vértices adjacentes a v, v_1, v_2,...,v_k. Retirando-se as arestas $\{v, v_1\}$, ..., $\{v, v_k\}$, como o grafo é acíclico, obtém-se $k + 1$ grafos (componentes) sem vértices em comum, k grafos em que estão os vértices v_1, v_2,...,v_k, e um contendo apenas v. Pela hipótese de indução, (c) vale para cada um deles. Com a reinclusão de v e arestas incidentes, haverá também um caminho simples de cada vértice de cada um dos $k + 1$ componentes a qualquer outro de outro componente, passando por v.

(c)→(a) A prova será feita por indução sobre o número de vértices. Se o grafo tem 1 vértice, ele não tem aresta, pois existe um único caminho simples do vértice a ele mesmo. Seja $n \geq 1$, e suponha que (a) vale para grafos (que satisfazem (c)) de n vértices ou menos. Seja Seja um grafo G de $n+1$ vértices que satisfaça (c). Seja v um vértice arbitrário de G de grau 1; v existe, pois o conjunto de vértices é finito e , assim, partindo-se de qualquer vértice, um caminhamento qualquer deve terminar antes repetir um vértice; caso contrário, existiria mais de um caminho simples, contrariando (c). Removendo-se v e a aresta incidente, obtém-se um grafo que, pela hipótese de indução, é uma árvore. Adicionando-se v e a aresta incidente, obtém-se então uma árvore.

1.10 Linguagens Formais

1. O número de prefixos e o de sufixos é $n+1$. O número máximo de subpalavras é $1 + C(n-1+2, 2) = 1 + C(n+1, 2) = 1 + (n+1)n/2$; assim, o número de subpalavras vai de $n+1$ a $1 + (n+1)n/2$.

2. a) $\{\mathtt{1}\}^*\{\mathtt{0}\}\{\mathtt{0},\mathtt{1}\}^*$.
   b) $\{\mathtt{0},\mathtt{1}\}(\{\mathtt{0},\mathtt{1}\}^2)^*$.
   c) $\{\mathtt{0}\}^*\{\mathtt{0}\}\{\mathtt{1}\}^*$.
   d) $\{\lambda\} \cup \{\mathtt{0}\}\{\mathtt{10}\}^* \cup \{\mathtt{1}\}\{\mathtt{01}\}^*$.
   e) $\{xx \mid x \in \{\mathtt{0},\mathtt{1}\}^*\}$.

3. a) $\{\mathtt{0},\mathtt{1}\}^{10}$.
   b) $\{\mathtt{0},\mathtt{1}\}\{\lambda,\mathtt{0},\mathtt{1}\}^{199}$.
   c) $\{\mathtt{01},\mathtt{1}\}\{\mathtt{0},\mathtt{1}\}^*\{\mathtt{00}\}$.
   d) $\{\mathtt{1},\mathtt{011}\}^*$.
   e) $\{\mathtt{1}\}^*(\{\mathtt{0}\}\{\mathtt{1}\}^*\{\mathtt{0}\}\{\mathtt{1}\}^*)^* \cup \{\mathtt{0}\}^*\{\mathtt{1}\}\{\mathtt{0}\}^*(\{\mathtt{1}\}\{\mathtt{0}\}^*\{\mathtt{1}\}\{\mathtt{0}\}^*)^*$.
   f) $\{\mathtt{0}\}^*\{\mathtt{1}\}\{\mathtt{0}\}^*\{\lambda,\mathtt{1}\}\{\mathtt{0}\}^* \cap (\{\mathtt{0},\mathtt{1}\}^3)^*$

4. a) $A(B \cup C) \subseteq (AB) \cup (AC)$
   Seja $w \in \Sigma^*$ tal que $w \in A(B \cup C)$. Então existem x e y tais que $w = xy$, $x \in A$ e $y \in B \cup C$. No caso em que $y \in B$, segue-se que $xy \in AB$ e no caso em que $y \in C$, segue-se que $xy \in AC$. Logo, $xy = w \in (AB) \cup (AC)$.
   $(AB) \cup (AC) \subseteq A(B \cup C)$
   Seja $w \in \Sigma^*$ tal que $w \in (AB) \cup (AC)$. Então $w \in AB$ ou $w \in AC$. No primeiro caso, existem x e y tais que $w = xy$, $x \in A$ e $y \in B$. Como $y \in B \cup D$ para qualquer linguagem D, segue-se que $xy = w \in A(B \cup C)$. No caso em que $w \in AC$, existem x e y tais que $w = xy$, $x \in A$ e $y \in C$. Como $y \in D \cup C$ para qualquer linguagem D, segue-se que $xy = w \in A(B \cup C)$. Conclui-se, portanto, que $w \in A(B \cup C)$.
   b) Contra-exemplo: $A = \{\lambda, a\}$, $B = \{b\}$, $C = \{ab\}$.

5. Suponha que $\lambda \in L$. Neste caso, $\lambda \in L^+$ e, portanto, $L^+ \cup \{\lambda\} = L^+$. Como $L^* = L^+ \cup \{\lambda\}$, segue-se que $L^* = L^+$. Agora suponha que $\lambda \notin L$. Então $\lambda \notin L^+$. Como $L^* = L^+ \cup \{\lambda\}$, segue-se que $L^+ = L^* - \{\lambda\}$.

6. L^* é finita se, e somente se, $L = \emptyset$ ou $L = \{\lambda\}$.

7. Uma condição necessária e suficiente para $L = L^R$ é: $w \in L$ se, e somente se, $w^R \in L$, para toda palavra w.

   Prova:

   $(\rightarrow)$ Suponha que $L = L^R$. Seja w uma palavra arbitrária. Se $w \in L$, então, pela definição de reverso, $w^R \in L^R$; e como $L^R = L$, $w^R \in L$. Por outro lado, se $w^R \in L$, então, pela definição de reverso, $(w^R)^R = w \in L^R$; e como $L^R = L$, $w \in L$. Assim, para toda palavra w, $w \in L$ se, e somente se, $w^R \in L$.

   $(\leftarrow)$ Suponha que $w \in L$ se, e somente se, $w^R \in L$, para toda palavra w. $L \subseteq L^R$, pois: se $x \in L$, então, pela suposição acima, $x^R \in L$; e pela definição de reverso, $(x^R)^R = x \in L^R$. Por outro lado, $L^R \subseteq L$, pois: se $x \in L^R$, da definição de reverso, tem-se que $x^R \in L$ (pois $x = (x^R)^R$); e pela suposição acima, $x \in L$. Conclui-se então que $L = L^R$.

8. A prova será por indução sobre n. Para $n = 0$, tem-se: $(w^R)^0 = \lambda = \lambda^R = (w^0)^R$. Seja $n \geq 0$ e suponha que $(w^R)^n = (w^n)^R$. Segue-se que: $(w^R)^{n+1} = (w^R)^n w^R = (w^n)^R w^R$, pela hipótese de indução. E como $(w^n)^R w^R = (ww^n)^R = (w^{n+1})^R$, segue-se que $(w^R)^{n+1} = (w^{n+1})^R$.

9. $L^* \subseteq \bigcup_{n \in \mathbf{N}} L^n$.

   Por indução forte sobre $|w|$. Suponha, como hipótese de indução, que se $w \in L^*$ então $w \in \bigcup_{n \in \mathbf{N}} L^n$ para palavras de tamanho menor que um certo k arbitrário. Para mostrar que isto vale também para palavras de tamanho k, considera-se dois casos:

   $k = 0$. A única palavra de tamanho 0 é λ, e $\lambda \in \bigcup_{n \in \mathbf{N}} L^n$, pois $L^0 = \{\lambda\}$.

   $k > 0$. Seja w de tamanho k tal que $w \in L^*$. Pela definição de fecho de Kleene, pode-se dizer que $w = xy$, onde $x \in L^*$, $y \in L$ e $y \neq \lambda$. Pela hipótese de indução, $x \in \bigcup_{n \in \mathbf{N}} L^n$. Segue-se que $x \in L^i$ para algum $i \in \mathbf{N}$. Como $y \in L$, tem-se que $xy \in L^{i+1}$. Portanto, $w \in \bigcup_{n \in \mathbf{N}} L^n$.

   $\bigcup_{n \in \mathbf{N}} L^n \subseteq L^*$.

   Este resultado segue do fato de que para todo $n \geq 0$, $L^n \subseteq L^*$, fato este que será provado por indução sobre n. Inicialmente, note que $L^0 = \{\lambda\}$, e $\lambda \in L^*$ por definição. Seja n arbitrário e suponha que $L^n \subseteq L^*$. Como $L^{n+1} = L^n L$, e, pela hipótese de indução, $L^n \subseteq L^*$, segue-se, pela definição de fecho de Kleene, que $L^{n+1} \subseteq L^*$.

10. a) Seja w uma palavra arbitrária. Se $w \in L^*$, como $\lambda \in L^*$, segue-se que $w\lambda = w \in L^*L^*$. Para completar, será provado, por indução no tamanho de y que para quaisquer palavras $x, y \in L^*$, se $xy \in L^*L^*$ então $xy \in L^*$. Inicialmente, veja que se $x \in L^*$, $x\lambda = x \in L^*$. Seja $n \geq 0$ e suponha, como hipótese de indução, que se $xy \in L^*L^*$ então $xy \in L^*$ para palavras y de n ou menos símbolos. Seja y uma palavra arbitrária de L^* de $n+1$ símbolos e $x \in L^*$. Então, $y = y_1y_2$, onde $y_1 \in L^*$ e $y_2 \in L$, $y_2 \neq \lambda$. Assim, dado que $xy_1 \in L^*L^*$, pela hipótes de indução $xy_1 \in L^*$. Como $y_2 \in L$, segue-se que $(xy_1)y_2 = xy \in L^*$.

    b) Seja w uma palavra arbitrária. Se $w \in L^*$, como $\lambda \in (L^*)^*$, segue-se da definição de fecho de Kleene que $\lambda w \in (L^*)^*L^*$, ou seja, $w \in (L^*)^*$. Será provado, por indução no tamanho de w que para quaisquer palavras $w \in (L^*)^*$, $w \in L^*$. Inicialmente, veja que $\lambda \in L^*$. Seja $n \geq 0$ e suponha, como hipótese de indução, que se $x \in (L^*)^*$ então $x \in L^*$ para palavras x de n ou menos símbolos. Seja w uma palavra de $n+1$ símbolos. Suponha que $w \in (L^*)^*$. Então $w = xy$, onde $x \in (L^*)^*$ e $y \in L^*$, $y \neq \lambda$. Como $|x| \leq n$, segue-se pela hipótese de indução que $x \in L^*$. Assim, $xy \in L^*L^*$ e, do resultado do item (a), segue-se que $xy \in L^*$.

c) Seja w uma palavra arbitrária. Se $w \in (L_1 \cup L_2)^*$, como $\lambda \in L_1^*$, segue-se que $w\lambda = w \in (L_1 \cup L_2)^* L_1^*$. Será mostrado por indução no tamanho de y que para quaisquer palavras $x \in (L_1 \cup L_2)^*$ e $y \in L_1^*$, se $xy \in (L_1 \cup L_2)^* L_1^*$ então $xy \in (L_1 \cup L_2)^*$. Inicialmente, observe que $\lambda \in (L_1 \cup L_2)^*$. Seja $n \geq 0$ e suponha, como hipótese de indução, que se $xy \in (L_1 \cup L_2)^* L_1^*$ então $xy \in (L_1 \cup L_2)^*$ para palavras $y \in L_1^*$ de n ou menos símbolos. Seja $y \in L_1^*$ uma palavra de $n+1$ símbolos; assim, $y = y_1 y_2$, onde $y_1 \in L_1^*$ e $y_2 \in L_1$, $y_2 \neq \lambda$, e suponha que $xy \in (L_1 \cup L_2)^* L_1^*$. Então $xy_1 \in (L_1 \cup L_2)^* L_1^*$. Como $|y_1| \leq n$, segue-se pela hipótese de indução que $xy_1 \in (L_1 \cup L_2)^*$. Como $y_2 \in L_1$, $y_2 \in L_1 \cup L_2$. Assim, $(xy_1)y_2 = w \in (L_1 \cup L_2)^*$.

d) $(L_1 \cup L_2)^* \subseteq (L_1^* L_2^*)^*$.
Será provado, por indução no tamanho de w que para quaisquer palavras $w \in (L_1 \cup L_2)^*$, $w \in (L_1^* L_2^*)^*$. Tem-se: $\lambda \in (L_1^* L_2^*)^*$. Seja $n \geq 0$ e suponha, como hipótese de indução, que $z \in (L_1^* L_2^*)^*$ para palavras $z \in (L_1 \cup L_2)^*$ de n ou menos símbolos. Seja $w \in (L_1 \cup L_2)^*$ de $n+1$ símbolos. Então, $w = xy$, $y \neq \lambda$, $x \in (L_1 \cup L_2)^*$ e $y \in (L_1 \cup L_2)$. Pela hipótese de indução, $x \in (L_1^* L_2^*)^*$. Se $y \in L_1$, então $y \in L_1^*$ e, como $\lambda \in L_2^*$, $y\lambda = y \in L_1^* L_2^*$; logo, $xy = w \in (L_1^* L_2^*)^*$. Por outro lado, se $y \in L_2$, raciocínio análogo mostra que $xy = w \in (L_1^* L_2^*)^*$.
$(L_1^* L_2^*)^* \subseteq (L_1 \cup L_2)^*$.
Será provado, por indução no tamanho de w que para quaisquer palavras $w \in (L_1^* L_2^*)^*$, $w \in (L_1 \cup L_2)^*$. Tem-se: $\lambda \in (L_1 \cup L_2)^*$. Seja $n \geq 0$ e suponha, como hipótese de indução, que $z \in (L_1 \cup L_2)^*$ para palavras $z \in (L_1^* L_2^*)^*$ de n ou menos símbolos. Seja $w \in (L_1^* L_2^*)^*$ de $n+1$ símbolos. Então, $w = xy$, $y \neq \lambda$, $x \in (L_1^* L_2^*)^*$ e $y \in L_1^* L_2^*$. Pela hipótese de indução, $x \in (L_1 \cup L_2)^*$. Sejam $y_1 \in L_1^*$ e $y_2 \in L_2^*$ tais que $y = y_1 y_2$. Então $w = xy_1y_2 \in (L_1 \cup L_2)^* L_1^* L_2^*$. Aplicando-se o resultado do item (c) duas vezes, conclui-se que $w \in (L_1 \cup L_2)^*$.

11. $L_1 = \{\lambda, \mathtt{a}\}$, $L_2 = \{\mathtt{a}, \mathtt{aa}\}$.

12. a) Definição recursiva de $X = \{\mathtt{0}\}^*\{\mathtt{1}\}^*$:
    - $\lambda \in X$;
    - se $x \in X$ então $\mathtt{0}x \in X$ e $x\mathtt{1} \in X$.

    b) Definição recursiva de $Y = \{\mathtt{0}^n\mathtt{1}^n \mid n \in \mathbf{N}\}$:
    - $\lambda \in Y$;
    - se $x \in Y$ então $\mathtt{0}x\mathtt{1} \in Y$.

    c) Definição recursiva de $Z = \{w \in \{\mathtt{0}, \mathtt{1}\}^* \mid w \text{ contém } \mathtt{00}\}$:
    - $\mathtt{00} \in Z$;
    - se $x \in Z$ então $\mathtt{0}x, \mathtt{1}x, x\mathtt{0}, x\mathtt{1} \in Z$.

    d) Definição recursiva de $W = \{\mathtt{0}^0\mathtt{1}\mathtt{0}^1\mathtt{1}\mathtt{0}^2\mathtt{1}\ldots\mathtt{0}^n\mathtt{1} \mid n \in \mathbf{N}\}$:
    - $\mathtt{1}, \mathtt{101} \in W$;
    - se $x\mathtt{1}\mathtt{0}^n\mathtt{1} \in W$ então $x\mathtt{1}\mathtt{0}^n\mathtt{1}\mathtt{0}^{n+1}\mathtt{1} \in W$.

1.11 Gramáticas

1. Nas derivações abaixo estão grifadas as variáveis expandidas.

a) $A \Rightarrow \underline{B}B \Rightarrow \underline{B} \Rightarrow \lambda$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B} \Rightarrow \lambda$.

b) $A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}\underline{B}\mathtt{1}B \Rightarrow \mathtt{01}\underline{B} \Rightarrow \mathtt{01}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}B\mathtt{1}\underline{B} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{01}$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B}\mathtt{0}B\mathtt{1} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{01}$.
$A \Rightarrow B\underline{B} \Rightarrow B\mathtt{0}\underline{B}\mathtt{1} \Rightarrow \underline{B}\mathtt{01} \Rightarrow \mathtt{01}$.

c) $A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}\underline{B}\mathtt{1}B \Rightarrow \mathtt{01}\underline{B} \Rightarrow \mathtt{010}\underline{B}\mathtt{1} \Rightarrow \mathtt{0101}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}B\mathtt{1}\underline{B} \Rightarrow \mathtt{0}\underline{B}\mathtt{10}B\mathtt{1} \Rightarrow \mathtt{010}\underline{B}\mathtt{1} \Rightarrow \mathtt{0101}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}B\mathtt{1}\underline{B} \Rightarrow \mathtt{0}B\mathtt{10}\underline{B}\mathtt{1} \Rightarrow \mathtt{0}\underline{B}\mathtt{101} \Rightarrow \mathtt{0101}$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B}\mathtt{0}B\mathtt{1} \Rightarrow \mathtt{0}\underline{B}\mathtt{10}B\mathtt{1} \Rightarrow \mathtt{010}\underline{B}\mathtt{1} \Rightarrow \mathtt{0101}$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B}\mathtt{0}B\mathtt{1} \Rightarrow \mathtt{0}B\mathtt{10}\underline{B}\mathtt{1} \Rightarrow \mathtt{0}\underline{B}\mathtt{101} \Rightarrow \mathtt{0101}$.
$A \Rightarrow B\underline{B} \Rightarrow B\mathtt{0}\underline{B}\mathtt{1} \Rightarrow B\mathtt{01} \Rightarrow \mathtt{0}\underline{B}\mathtt{101} \Rightarrow \mathtt{0101}$.

d) $A \Rightarrow \underline{B}B \Rightarrow \underline{B} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}\underline{B}\mathtt{1}B \Rightarrow \mathtt{00}\underline{B}\mathtt{11}B \Rightarrow \mathtt{0011}\underline{B} \Rightarrow \mathtt{0011}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}\underline{B}\mathtt{1}B \Rightarrow \mathtt{00}B\mathtt{11}\underline{B} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow \underline{B}B \Rightarrow \mathtt{0}B\mathtt{1}\underline{B} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow B\underline{B} \Rightarrow \underline{B}\mathtt{0}B\mathtt{1} \Rightarrow \mathtt{0}\underline{B}\mathtt{1} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow B\underline{B} \Rightarrow B\mathtt{0}\underline{B}\mathtt{1} \Rightarrow \underline{B}\mathtt{00}B\mathtt{11} \Rightarrow \mathtt{00}\underline{B}\mathtt{11} \Rightarrow \mathtt{0011}$.
$A \Rightarrow B\underline{B} \Rightarrow B\mathtt{0}\underline{B}\mathtt{1} \Rightarrow B\mathtt{00}\underline{B}\mathtt{11} \Rightarrow \underline{B}\mathtt{0011} \Rightarrow \mathtt{0011}$.

A linguagem gerada é $\{\mathtt{0}^n\mathtt{1}^n \mid n \in \mathbf{N}\}^2$.

2. $L(G') = L(G)$. Cada palavra gerada por G, a gramática do Exemplo 49, pode ser gerada por uma derivação da forma:

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

Cada uma destas palavras pode ser gerada, por meio de G', como mostrado abaixo. O que está diferente está grifado.

$$
\begin{array}{lll}
P \Rightarrow & \mathtt{a}A\mathtt{b}\underline{D} & \text{(regra 1)} \\
\stackrel{k}{\Rightarrow} & \mathtt{aa}^k A(\mathtt{b}C)^k\mathtt{b}\underline{D} & \text{(regra 2, } k \text{ vezes; } k \geq 0) \\
\Rightarrow & \mathtt{aa}^k(\mathtt{b}C)^k\mathtt{b}\underline{D} & \text{(regra 3)} \\
\Rightarrow & \mathtt{a}^{k+1}(\mathtt{b}C)^{k-1}\mathtt{b}^2\mathtt{C}\underline{D} & \text{(regra 4, 1 vez)} \\
\stackrel{2}{\Rightarrow} & \mathtt{a}^{k+1}(\mathtt{b}C)^{k-2}\mathtt{b}^3\mathtt{C}^2\underline{D} & \text{(regra 4, 2 vezes)} \\
\vdots & & \\
\stackrel{k}{\Rightarrow} & \mathtt{a}^{k+1}\mathtt{b}^{k+1}\mathtt{C}^k\underline{D} & \text{(regra 4, } k \text{ vezes)} \\
\stackrel{k}{\Rightarrow} & \mathtt{a}^{k+1}\mathtt{b}^{k+1}\underline{D}c^k & \text{(regra 5, } k \text{ vezes)} \\
\stackrel{k}{\Rightarrow} & \mathtt{a}^{k+1}\mathtt{b}^{k+1}c^{k+1} & \text{(regra 6, 1 vez)}
\end{array}
$$

Note-se que uma derivação de uma palavra da linguagem gasta um passo a mais na gramática G': o último, que é usado para produzir o último $\mathtt{c}$. Uma derivação em G' que, usando a regra 6, substitua D por $\mathtt{c}$ antes da subsitituição de todos os Cs por $\mathtt{c}$s, não leva a nenhuma palavra da linguagem.

3. a) $P \rightarrow \mathtt{a}I \,|\, \mathtt{b}P \,|\, \lambda$
   $I \rightarrow \mathtt{a}P \,|\, \mathtt{b}I$

   b) $X \rightarrow \mathtt{a}X\mathtt{b} \,|\, \lambda$

   c) $X \rightarrow \mathtt{a}X\mathtt{a} \,|\, \mathtt{b}X\mathtt{b} \,|\, \lambda \,|\, \mathtt{a} \,|\, \mathtt{b}$

   d) $P \rightarrow A \,|\, B \,|\, \lambda$
   $A \rightarrow \mathtt{a}B\mathtt{a} \,|\, \mathtt{a}$
   $B \rightarrow \mathtt{b}A\mathtt{b} \,|\, \mathtt{b}$

   e) $P \rightarrow \mathtt{a}BPC\mathtt{d} \,|\, \lambda$
   $BC \rightarrow \mathtt{bc}$
   $B\mathtt{a} \rightarrow \mathtt{a}B$
   $B\mathtt{b} \rightarrow \mathtt{bb}$
   $\mathtt{d}C \rightarrow C\mathtt{d}$
   $\mathtt{c}C \rightarrow \mathtt{cc}$

4. Para a gramática do item (b), observando-se o esquema:

   $$X \stackrel{k}{\Rightarrow} \mathtt{a}^k X \mathtt{b}^k \Rightarrow \mathtt{a}^k\mathtt{b}^k.$$

   vê-se que são gastos $k + 1 = (n/2) + 1$ passos.

   Para a gramática do item (c), se $n = 0$, é gasto 1 passo:

   $$X \Rightarrow \lambda$$

   e se $n > 0$ são gastos $k = \lceil n/2 \rceil + 1$ passos, pois

   - Uma derivação começa assim: $X \stackrel{k}{\Rightarrow} xXx^R$ (regras 1 e 2, k vezes, $k \geq 0$, $|x| = |x^R| = k$).
   - Em seguida, é aplicada uma das 3 últimas regras. Se for a regra λ, o número de passos é $k = (n/2) + 1$, onde $n = 2k$. Se for uma das outras duas regras, o número de passos é $k = [(n-1)/2] + 1$, onde $n = 2k + 1$.

5. $L(G) = \{\mathtt{a}\}^*\{\mathtt{b}\}^*$.

   Prova:

   $\{\mathtt{a}\}^*\{\mathtt{b}\}^* \subseteq L(G)$. O seguinte esquema de derivação mostra que toda palavra da forma $\mathtt{a}^i\mathtt{b}^j$, para $i, j \geq 0$, é gerada por G:

   $$\begin{array}{rll} A & \stackrel{i}{\Rightarrow} \mathtt{a}^i A & (\text{regra } A \rightarrow \mathtt{a}A,\ i \text{ vezes},\ i \geq 0) \\ & \Rightarrow \mathtt{a}^i B & (\text{regra } A \rightarrow B) \\ & \stackrel{j}{\Rightarrow} \mathtt{a}^i\mathtt{b}^j B & (\text{regra } B \rightarrow \mathtt{b}B,\ j \text{ vezes},\ j \geq 0) \\ & \Rightarrow \mathtt{a}^i\mathtt{b}^j & (\text{regra } B \rightarrow \lambda) \end{array}$$

   Como *qualquer palavra* gerada por G segue necessariamente este mesmo esquema de derivação, segue-se que $L(G) \subseteq \{\mathtt{a}\}^*\{\mathtt{b}\}^*$.

1.12 Problemas de Decisão

1. a) Nada se pode dizer. X pode ser decidível ou não.

   b) X é decidível: para qualquer entrada x (para X), o algoritmo $\mathcal{R}$ produz uma saída y, a partir da qual um algoritmo para D obtém a resposta para x.

   c) X é indecidível: pelo item anteriror, se X fosse decidível, I seria decidível.

   d) Nada se pode dizer. X pode ser decidível ou não.

1.13 Exercícios

1. Segue uma definição recursiva de $\hat{v}$: LP $\rightarrow \{V, F\}$:

   a) $\hat{v}(\alpha) = v(\alpha)$ para $\alpha \in$ VP;

   b) $\hat{v}(\neg\alpha) = V$ se, e somente se, $\hat{v}(\alpha) = F$;
   $\hat{v}((\alpha \wedge \beta)) = V$ se, e somente se, $\hat{v}(\alpha) = V$ e $\hat{v}(\beta) = V$;
   $\hat{v}((\alpha \vee \beta)) = F$ se, e somente se, $\hat{v}(\alpha) = F$ e $\hat{v}(\beta) = F$;
   $\hat{v}((\alpha \rightarrow \beta)) = F$ se, e somente se, $\hat{v}(\alpha) = V$ e $\hat{v}(\beta) = F$;
   $\hat{v}((\alpha \leftrightarrow \beta)) = V$ se, e somente se, $\hat{v}(\alpha) = \hat{v}(\beta)$.

2. Basta substituir, indutivamente:

   - $\alpha \wedge \beta$ por $\neg(\neg\alpha \vee \neg\beta)$;
   - $\alpha \rightarrow \beta$ por $\neg\alpha \vee \beta$;
   - $\alpha \leftrightarrow \beta$ por $(\neg\alpha \vee \beta) \wedge (\alpha \vee \neg\beta)$;
   - $\exists x\alpha$ por $\neg\forall x\neg\alpha$.

3. Por indução sobre n. Inicialmente, veja que $(0 + 1)^2 - 0^2 = 1 > 0$. Seja n um número natural arbitrário. Suponha, como hipótese de indução, que existe $k \in \mathbf{N}$ tal que $(k+1)^2 - k^2 > n$. Seja k_0 tal número. Como $(k_0+1)^2-k_0^2 = k_0^2+2k_0+1-k_0^2 = 2k_0+1$, pela hipótese de indução, tem-se que $2k_0 + 1 > n$. Logo, $2k_0 + 2 > n + 1$. E como $(k_0 + 2)^2 - (k_0 + 1)^2 = k_0^2 + 4k_0 + 4 - k_0^2 - 2k_0 - 1 = 3k_0 + 3$, segue-se que $(k_0 + 2)^2 - (k_0 + 1)^2 > n + 1$. Portanto, existe um número natural k tal que $(k + 1)^2 - k^2 > n + 1$: $k_0 + 1$ seria um tal número.

4. Deve-se provar que existem $k, n_0 \in \mathbf{N}$ tais que para todo $n \geq n_0$, $10n^2+100n+1000 \leq kn^2$. Sejam $k = 1110$ e $n_0 = 1$. Será provado, por indução, que para todo $n \geq n_0$, $10n^2+100n+1000 \leq kn^2 = 1110n^2$. Inicialmente, veja que $10 \times 1^2 + 100 \times 1 + 1000 = 1110 = 1110 \times 1^2$. Seja n um número natural arbitrário maior ou igual a 1, e suponha, como hipótese de indução, que $10n^2 + 100n + 1000 \leq 1110n^2$. Segue-se que $10(n+1)^2 + 100(n+1) + 1000 = 10n^2 + 20n + 10 + 100n + 100 + 1000 = (10n^2 + 100n + 1000) + 20n + 110$. Pela hipótese de indução, $(10n^2 + 100n + 1000) + 20n + 110 \leq 1110n^2 + 20n + 110$. Como esta última é menor do que $(1110n^2 + 20n + 110) + 2200n + 1000$ e esta, por sua vez é igual a $1110n^2 + 2220n+1110 = 1110(n+1)^2$, conclui-se que $10(n+1)^2+100(n+1)+1000 < 1110(n+1)^2$. Portanto, pelo princípio de indução, para todo $n \geq 1$, $10n^2 + 100n + 1000 \leq 1110n^2$. Já que existem $k, n_0 \in \mathbf{N}$ tais que para todo $n \geq n_0$, $10n^2 + 100n + 1000 \leq kn^2$, conclui-se que $10n^2 + 100n + 1000$ é $O(n^2)$.

   Técnicas de provas utilizadas: construtiva para a existencial 2 vezes (quando se exibiu $k = 1110$ e $n_0 = 1$) e indução (para provar que para todo $n \geq n_0 \ldots$).

5. $|A \cup B| = |A| + |B| - |A \cap B|$. *Prova*: Cada elemento de $A - B$ e cada elemento de $A \cap B$ é contado uma vez em $|A|$, e cada elemento de $B - A$ e cada elemento de $A \cap B$ é contado uma vez em $|B|$. Assim, os elementos de $A \cap B$ são contados duas vezes em $|A| + |B|$, razão da subtração de $|A \cap B|$.

   Generalizando: $|\cup_{i=1}^{n} A_i| = S_1 + S_2 + \cdots + S_n$, onde:

$$S_k = (-1)^{k+1} \times \sum_{j_1 \neq j_2 \neq \cdots \neq j_k} |A_{j_1} \cap A_{j_2} \cap \ldots \cap A_{j_k}|, \text{ para } 1 \leq k \leq n.$$

   Para provar este resultado por indução, note inicialmente que $|\cup_{i=1}^{1} A_i| = |A_1| = S_1$. Seja $n \geq 1$ arbitrário. Hipótese de indução: $|\cup_{i=1}^{n} A_i| = S_1 + S_2 + \cdots + S_n$, sendo S_k definido como acima. Basta, agora, provar que $|\cup_{i=1}^{n+1} A_i| = S'_1 + S'_2 + \cdots + S'_{n+1}$, onde cada S'_k é como S_k, só que cada j_k pode ser também $k+1$. Como $\cup_{i=1}^{n+1} A_i = (\cup_{i=1}^{n} A_i) \cup A_{n+1}$, tem-se, pelo resultado acima, que:

$$|\cup_{i=1}^{n+1} A_i| = |\cup_{i=1}^{n} A_i| + |A_{n+1}| - |(\cup_{i=1}^{n} A_i) \cap A_{n+1}|.$$

   Pela hipótese de indução, segue-se que:

$$|\cup_{i=1}^{n+1} A_i| = S_1 + S_2 + \cdots + S_n + |A_{n+1}| - |(\cup_{i=1}^{n} A_i) \cap A_{n+1}|.$$

   Como $S'_1 = S_1 + |A_{n+1}|$ e a interseção distribui sobre união:

$$|\cup_{i=1}^{n+1} A_i| = S'_1 + S_2 + \cdots + S_n - |\cup_{i=1}^{n} (A_i \cap A_{n+1})|.$$

   Pela hipótese de indução, tem-se que:

$$|\cup_{i=1}^{n+1} (A_i \cap A_{n+1})| = S''_1 + S''_2 + \cdots + S''_n, \text{ onde:}$$

$$S''_k = (-1)^{k+1} \times \sum_{j_1 \neq j_2 \neq \cdots \neq j_k} |(A_{j_1} \cap A_{n+1}) \cap (A_{j_2} \cap A_{n+1}) \cap \ldots \cap (A_{j_k} \cap A_{n+1})|$$

   para $1 \leq k \leq n$. Ou ainda:

$$S''_k = (-1)^{k+1} \times \sum_{j_1 \neq j_2 \neq \cdots \neq j_k} |A_{j_1} \cap A_{j_2} \cap \ldots \cap A_{j_k} \cap A_{n+1}|.$$

   Assim, como

$$|\cup_{i=1}^{n+1} A_i| = S'_1 + S_2 + \cdots + S_n - (S''_1 + S''_2 + \cdots + S''_n).$$

   e como $S_2 - S''_1 = S'_2$, $S_3 - S''_2 = S'_3$, $\ldots$, $S_n - S''_{n-1} = S'_n$, e $-S''_n = S'_{n+1}$, conclui-se que $|\cup_{i=1}^{n+1} A_i| = S'_1 + S'_2 + \cdots + S'_n + S'_{n+1}$.

6. a) Seja X um elemento arbitrário de $\mathcal{P}(A) \cup \mathcal{P}(B)$. Então $X \in \mathcal{P}(A)$ ou $X \in \mathcal{P}(B)$. No primeiro caso, $X \subseteq A$, e no segundo, $X \subseteq B$. Em qualquer caso, $X \subseteq A \cup B$. Portanto, $X \in \mathcal{P}(A \cup B)$. Conclui-se que $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

   b) $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.
   Seja X um elemento arbitrário de $\mathcal{P}(A) \cap \mathcal{P}(B)$. Então $X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$; logo, $X \subseteq A$ e $X \subseteq B$. Segue-se que $X \subseteq A \cap B$. Portanto, $X \in \mathcal{P}(A \cap B)$. Conclui-se que $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.
   $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.
   Seja X um elemento arbitrário de $\mathcal{P}(A \cap B)$. Então $X \subseteq A \cap B$; logo, $X \subseteq A$ e $X \subseteq B$. Segue-se que $X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$. Portanto, $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Conclui-se que $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

7. a) $A \triangle B \subseteq (A \cup B) - (A \cap B)$.

Seja $x \in A \triangle B$. Então, por definição, $x \in A - B$ ou $x \in B - A$. No primeiro caso, $x \in A$ e $x \notin B$; como $x \in A$, $x \in A \cup B$, e como $x \notin B$, $x \notin A \cap B$. Assim, $x \in (A \cup B) - (A \cap B)$. No segundo caso, procede-se de forma análoga para mostrar que também $x \in (A \cup B) - (A \cap B)$.

$(A \cup B) - (A \cap B) \subseteq A \triangle B$.

Seja $x \in (A \cup B) - (A \cap B)$. Segue-se que $x \in A \cup B$ e $x \notin A \cap B$. *Caso 1:* $x \in A$. Como $x \notin A \cap B$, $x \notin B$. Assim, $x \in A - B$. *Caso 2:* $x \in B$. Como $x \notin A \cap B$, $x \notin A$. Assim, $x \in B - A$. Portanto, $x \in A - B$ ou $x \in B - A$, ou ainda, $x \in (A - B) \cup (B - A) = A \triangle B$.

b) $A \triangle (B \triangle C) \subseteq (A \triangle B) \triangle C$.

Seja $x \in A \triangle (B \triangle C)$. Então, pela definição, $x \in A - (B \triangle C)$ ou $x \in (B \triangle C) - A$.
<u>Caso 1:</u> $x \in A - (B \triangle C)$.
Então $x \in A$ e $x \notin B \triangle C$. Desta última, segue-se que $x \notin B - C$ e $x \notin C - B$, ou seja, (I) $x \notin B$ ou $x \in C$ e (II) $x \notin C$ ou $x \in B$. Por um lado, se $x \in C$, de (II) segue-se que $x \in B$; com isto, $x \notin A - B$ e $x \notin B - A$; logo, $x \notin A \triangle B$ e, assim, $x \in C - A \triangle B$. Por outro lado, se $x \notin C$, de (I) segue-se $x \notin B$; com isto, e como $x \in A$, $x \in A - B$ e, portanto, $x \in A \triangle B$; segue-se que $x \in (A \triangle B) - C$. Como $x \in C - A \triangle B$ se $x \in C$, e $x \in (A \triangle B) - C$ se $x \notin C$, conclui-se que $x \in (A \triangle B) \triangle C$.
<u>Caso 2:</u> $x \in (B \triangle C) - A$
Então $x \in B \triangle C$ e $x \notin A$. Da primeira, Segue-se que $x \in B$ e $x \notin C$ ou $x \in C$ e $x \notin B$. No caso em que $x \in B$ e $x \notin C$, $x \in B - A$ e, portanto, $x \in A \triangle B$; segue-se que $x \in (A \triangle B) - C$ e que $x \in (A \triangle B) \triangle C$. E no caso em que $x \in C$ e $x \notin B$, $x \notin A - B$ e $x \notin B - A$; portanto, $x \notin A \triangle B$; e assim, $x \in C - (A \triangle B)$, ou ainda, $x \in (A \triangle B) \triangle C$.

$(A \triangle B) \triangle C \subseteq A \triangle (B \triangle C)$.

Procede-se forma similar à acima.

c) $(A - B) \triangle (B - A) \subseteq A \triangle B$.

Seja $x \in (A - B) \triangle (B - A)$. Então $x \in (A - B) - (B - A)$ ou $x \in (B - A) - (A - B)$. No caso em que $x \in (A - B) - (B - A)$, $x \in A - B$ e, portanto, $x \in A \triangle B$. E no caso em que $x \in (B - A) - (A - B)$, $x \in A - B$ e, portanto, $x \in A \triangle B$.

$A \triangle B \subseteq (A - B) \triangle (B - A)$.

Seja $x \in A \triangle B$. Então $x \in A - B$ ou $x \in B - A$. No primeiro caso, segue-se que $x \in (A - B) - (B - A)$, e no segundo segue-se que $x \in (B - A) - (A - B)$. Assim, em qualquer caso, $x \in (A - B) \triangle (B - A)$.

d) $(\rightarrow)$

Suponha que $A \triangle B = A$ e suponha que $B \neq \emptyset$. Seja, então $b \in B$. Se $b \in A$, então, como $A \triangle B = A$, $b \in A \triangle B$; mas isto é impossível, pois se $b \in A$, $b \notin B - A$ e se $b \in B$, $b \notin A - B$. Assim, $b \notin A$. Neste caso, $b \in B - A$ e, logo, $b \in A \triangle B$. Mas isto também nõ pode ser, já que $A \triangle B = A$. Conclui-se, portanto, que b não pode existir, e, assim, $B = \emptyset$.

$(\leftarrow)$

Suponha que $B = \emptyset$. Prova-se, primeiro, que $A \triangle B \subseteq A$. Seja $x \in A \triangle B$. Com isto, $x \in A - B$ ou $x \in B - A$. Como $B = \emptyset$, este último caso é impossível. Assim, $x \in A - B$. E como $B = \emptyset$, $x \in A$. Portanto, $A \triangle B \subseteq A$. Agora, prova-se que $A \subseteq A \triangle B$. Seja $x \in A$. Como $B = \emptyset$, $x \in A - B$ e, portanto, $x \in A \triangle B$. Logo, $A \subseteq A \triangle B$.

e) $A - B = A \triangle B$ se, e somente se, $B \subseteq A$, como provado abaixo.

($\rightarrow$)

Suponha que $A - B = A \triangle B$. Seja $b \in B$. Com isto, $b \notin A - B$. Supondo que $b \notin A$, segue-se que $b \in B - A$ e, portanto, $b \in A \triangle B$. Isto não pode ser, visto que $A - B = A \triangle B$. Assim, se $b \in B$, então $b \in A$. Portanto, $B \subseteq A$.

($\leftarrow$)

Suponha que $B \subseteq A$. Se $x \in A - B$, então $x \in A \triangle B$; logo $A - B \subseteq A \triangle B$. Assim, basta mostrar que $A \triangle B \subseteq A - B$. Seja $x \in A \triangle B$. Como $B \subseteq A$, tem-se $x \notin B - A$; portanto, $x \in A - B$. Logo, $A \triangle B \subseteq A - B$.

8. Seja uma relação R reflexiva e transitiva arbitrária. Será mostrado por indução que $R^n = R$ para todo $n \geq 1$. $R^1 = R$, por definição. Seja $n \geq 1$. Suponha, como hipótese de indução, que $R^n = R$. Por definição, $R^{n+1} = R^n \circ R$, pois $n + 1 \geq 2$. Pela hipótese de indução, $R^n = R$. Assim, basta mostrar que $R \circ R = R$. Mostra-se primeiro que $R \subseteq R \circ R$. Para isto, seja $(x, y) \in R$. Como R é reflexiva, $(x, x) \in R$. Logo, $(x, y) \in R \circ R$. Portanto, $R \subseteq R \circ R$. Agora, mostra-se que $R \circ R \subseteq R$. Seja $(x, y) \in R \circ R$; então existe z tal que $(x, z) \in R$ e $(z, y) \in R$. Como R é transitiva, $(x, y) \in R$. Portanto, $R \circ R \subseteq R$.

9. Seja $F : A \rightarrow A$ tal que $f(a) = a_C$ para todo $a \in A$, onde a_C é um certo elemento da classe de equivalência a que pertence a. Tal elemento existe, visto que todo $a \in A$ pertence a alguma classe de equivalência e classes de equivalência não são vazias. Qualquer elemento da classe de equivalência de a serve para ser a_C, mas escolhido um, ele deve ser a única imagem para todos os componentes da classe. Uma função assim satisfaz os requisitos, como mostrado abaixo.

   ($\rightarrow$)

   Suponha que xRy. Então x e y pertencem à mesma classe de equivalência C e, portanto, $f(x) = x_C = y_C = f(y)$.

   ($\leftarrow$)

   Suponha que $f(x) = f(y)$. Então $f(x)$ e $f(y)$ pertencem à mesma classe de equivalência. Portanto, xRy.

10. $[a] \neq \emptyset$, visto que R é reflexiva e, portanto, aRa.

    Agora, mostra-se que as classes de equivalência são disjuntas, ou seja, dados $a, b \in A$, $[a] = [b]$ ou $[a] \cap [b] = \emptyset$. Suponha que $[a] \cap [b] \neq \emptyset$, e seja $x \in A$ tal que $x \in [a]$ e $x \in [b]$. Seja $y \in [a]$. Então, aRy e, por simetria, yRa. Como aRx, por transitividade, yRx. Como xRb, por transitividade, yRb. Por simetria, bRy. Logo, $y \in [b]$. Como y é um elemento arbitrário de $[a]$, $[a] \subseteq [b]$. De form análoga, mostra-se $[b] \subseteq [a]$.

    Falta mostrar que $\cup_{a \in A}[a] = A$. As classes de equivalência $[a]$ só têm elementos de A. Assim, $\cup_{a \in A}[a] \subseteq A$. Por outro lado, se $x \in A$, então existe uma classe de equivalência $[x]$ por definição, o que mostra que $A \subseteq \cup_{a \in A}[a]$.

11. a) $f(A \cup B) \subseteq f(A) \cup f(B)$.

    Seja $x \in f(A \cup B)$. Então, $x = f(y)$ onde $y \in A \cup B$. Se $y \in A$, segue-se que $f(y) \in f(A)$ e se $y \in B$, $f(y) \in f(B)$. Assim, $x = f(y) \in f(A) \cup f(B)$.

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

    Seja $x \in f(A) \cup f(B)$. Então $x \in f(A)$ ou $x \in f(B)$. Se $x \in f(A)$, então $x = f(y)$, onde $y \in A$; se $y \in A$, $y \in A \cup B$, e portanto $x = f(y) \in f(A \cup B)$. Da mesma forma, mostra-se que se $x \in f(B)$, $x \in f(A \cup B)$.

b) $f(A \cap B) \subseteq f(A) \cap f(B)$.
Seja $x \in f(A \cap B)$. Então, $x = f(y)$ onde $y \in A \cap B$. Assim, $y \in A$ e $y \in B$, de onde se segue que $f(y) \in f(A)$ e $f(y) \in f(B)$. Logo, $x = f(y) \in f(A) \cap f(B)$.

12. a) Tem-se:

$$\begin{aligned} f_A(x) = 1 &\leftrightarrow x \in A && \text{por definição} \\ &\leftrightarrow x \notin \overline{A} \\ &\leftrightarrow f_{\overline{A}}(x) \neq 1 && \text{por definição} \\ &\leftrightarrow f_{\overline{A}}(x) = 0 \\ &\leftrightarrow 1 - f_{\overline{A}}(x) = 1. \end{aligned}$$

Portanto, $f_A(x) = 1 - f_{\overline{A}}(x)$.

b) Tem-se:

$$\begin{aligned} f_{A\cup B}(x) = 1 &\leftrightarrow x \in A \cup B && \text{por definição} \\ &\leftrightarrow x \in A \text{ ou } x \in B \\ &\leftrightarrow f_A(x) = 1 \text{ ou } f_B(x) = 1 && \text{por definição} \\ &\leftrightarrow f_A(x) + f_B(x) - f_A(x)f_B(x) = 1. \end{aligned}$$

Portanto, $f_{A\cup B}(x) = f_A(x) + f_B(x) - f_A(x)f_B(x)$.

c) Tem-se:

$$\begin{aligned} f_{A\cap B}(x) = 1 &\leftrightarrow x \in A \cap B && \text{por definição} \\ &\leftrightarrow x \in A \text{ e } x \in B \\ &\leftrightarrow f_A(x) = 1 \text{ e } f_B(x) = 1 && \text{por definição} \\ &\leftrightarrow f_A(x)f_B(x) = 1. \end{aligned}$$

Portanto, $f_{A\cap B}(x) = f_A(x)f_B(x)$.

d) Tem-se:

$$\begin{aligned} f_{A-B}(x) = 1 &\leftrightarrow x \in A - B && \text{por definição} \\ &\leftrightarrow x \in A \text{ e } x \notin B \\ &\leftrightarrow f_A(x) = 1 \text{ e } f_B(x) \neq 1 && \text{por definição} \\ &\leftrightarrow f_A(x) = 1 \text{ e } f_B(x) = 0 \\ &\leftrightarrow f_A(x) = 1 \text{ e } 1 - f_B(x) = 1 \\ &\leftrightarrow f_A(x)(1 - f_B(x)) = 1. \end{aligned}$$

Portanto, $f_{A\cap B}(x) = f_A(x)f_B(x)$.

13. $(\rightarrow)$

Seja uma função injetora $f : A \rightarrow B$. Seja C a imagem de A. Então $g : C \rightarrow A$ tal que $g(c)$ é o elemento a tal que $f(a) = c$ é uma função sobretora. O elemento a existe e é único visto que f é uma função injetora.

$(\leftarrow)$

Seja uma função sobrejetora $f : B \rightarrow A$. Então $g : A \rightarrow B$ tal que $g(a)$ é algum elemento de $\{b \,|\, f(b) = a\}$ é uma função injetora. Como f é uma função sobrejetora, para todo a tal conjunto não é vazio; e os conjuntos são disjuntos, pois f é função.

14. Seja $\Sigma = \{a_1, a_2, \ldots, a_n\}$. Então:

Σ^* **é enumerável.** Uma enumeração para Σ é dada pela função $\eta : \Sigma^* \rightarrow \mathbf{N}$ tal que $\eta(\lambda) = 0$ e $\eta(a_{p_m} a_{p_{m-1}} \ldots a_{p_0}) = \sum_{k=0}^{m}(p_k \times n^k)$.

$\mathcal{P}(\Sigma^*)$ **não é enumerável.** Suponha que $\mathcal{P}(\Sigma^*)$ é enumerável. Então existe uma função bijetora de $\mathcal{P}(\Sigma^*)$ para $\mathbf{N}$, de forma que os elementos de $\mathcal{P}(\Sigma^*)$ podem ser enumerados: $A_0, A_1, A_2, \ldots$. Seja o conjunto $B = \{w \in \Sigma^* \,|\, w \notin A_{\eta(w)}\}$, onde η é a função de enumeração vista acima (ou qualquer outra). Mas, como $\{\eta(w) \,|\, w \in \Sigma^*\} = \mathbf{N}$, segue-se que $B \neq A_i$ para todo $i \in \mathbf{N}$. Logo, a suposição de que existe a enumeração $A_0, A_1, A_2, \ldots$ não é correta, ou seja, $\mathcal{P}(\Sigma^*)$ não é enumerável.

15. Seja uma função bijetora $f : A \to \mathcal{P}(A)$. Agora, considere o conjunto $D \subseteq A$ assim definido:

$$\text{para cada } a \in A, a \in D \text{ se, e somente se, } a \notin f(a).$$

Como f é uma função bijetora, para cada $X \subseteq A$ deve existir $x \in A$ tal que $f(x) = X$. Em particular, para D deve então existir $d \in A$ tal que $f(d) = D$. Mas, pela definição de D, segue-se que $d \in D = f(d)$ se, e somente se, $d \notin f(d)$. Tal contradição leva à conclusão que não existe uma função bijetora de um conjunto A para um conjunto $\mathcal{P}(A)$.

Este resultado implica que para qualquer conjunto existe conjunto com cardinalidade maior. Em particular, considerando-se conjuntos infinitos, existe uma infinidade de "ordens de infinidade": $\mathbf{N}$, $\mathcal{P}(\mathbf{N})$, $\mathcal{P}(\mathcal{P}(\mathbf{N}))$, etc.

16. A representação de um número n na base b gasta $\lfloor \log_b n \rfloor + 1$ símbolos, se $b > 1$. Como $\log_b n = \log_b c \times \log_c n$, onde $b > 1$ e $c > 1$, vê-se que a transição de uma base para outra, ambas maiores ou iguais a 2, é influenciada apenas por um fator constante, $\log_b c$. E dado o exposto no Exemplo 47, as representações em bases maiores ou iguais a 2 são exponencialmente mais concisas do que na base 1.

17. Definição recursiva de $v : \{\mathtt{0}, \mathtt{1}\}^* \to \mathbf{N}$, de forma que $v(w)$ é o número representado por w na base 2:

    a) $v(\mathtt{0}) = 0$ e $v(\mathtt{1}) = 1$;

    b) $v(x\mathtt{0}) = 2v(x)$ e $v(x\mathtt{1}) = 2v(x) + 1$.

18. Subtração:

    a) $m - 0 = m$, para todo $m \in \mathbf{N}$;

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

    Divisão:

    a) $m/s(0) = m$, para todo $m \in \mathbf{N}$;

    b) para todo $m \in \mathbf{N}$ e todo $n > s(0)$, $m/n = 0$, se $m < n$, e $m/n = s((m-n)/n)$, se $m \geq n$.

    onde a relação $<$ é assim definida:

    a) $n < s(n)$, para todo $n \in \mathbf{N}$;

    b) se $m < n$, então $m < s(n)$, para todo $m, n \in \mathbf{N}$.

    Resto da divisão:

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

    b) $m \, mod \, n = m$, se $m < n$;

    c) $m \, mod \, n = (m - n) \, mod \, n$, se $n < m$.

Máximo divisor comum:

a) $mdc(n, n) = n$, para todo $n \in \mathbf{N}$;
b) $mdc(m, n) = mdc(m - n, n)$, se $n < m$;
c) $mdc(m, n) = mdc(m, n - m)$, se $m < n$.

19. Conjunto $Anc(v)$ de ancestrais de um vértice v de uma árvore (V, A, r):

a) $v \in Anc(v)$;
b) se $v \in Anc(v)$ e $(v', v) \in A$, então $v' \in Anc(v)$.

20. $\psi(n) = \lfloor \log_2 n \rfloor$. Será feita uma demonstração por indução forte. Assim, suponha, como hipótese de indução, que $\psi(k) = \lfloor \log_2 k \rfloor$ para todo $k < n$.
<u>Caso $n = 1$</u>. $\psi(1) = 0 = \log_2 1$.
<u>Caso $n > 1$</u>. Por definição, $\psi(n) = \psi(\lfloor n/2 \rfloor)+1$. Como, $\lfloor n/2 \rfloor < n$, segue-se, pela hipótese de indução, que $\psi(n) = \lfloor \log_2 \lfloor n/2 \rfloor \rfloor + 1$. Se $n \; mod \; 2 = 0$, então $\psi(n) = \lfloor \log_2 n/2 \rfloor + 1 = \lfloor (\log_2 n) - 1 \rfloor + 1 = \lfloor (\log_2 n) \rfloor - 1 + 1 = \lfloor \log_2 n \rfloor$. Por outro lado, se $n \; mod \; 2 = 1$, então $\psi(n) = \lfloor \log_2 (n-1)/2 \rfloor + 1 = \lfloor \log_2 (n-1) - 1 \rfloor + 1 = \lfloor \log_2 (n-1) \rfloor - 1 + 1 = \lfloor \log_2 (n-1) \rfloor$. Mas, se $n \; mod \; 2 = 1$ e $n > 0$, $\lfloor \log_2 (n - 1) \rfloor = \lfloor \log_2 n \rfloor$. Assim, $\psi(n) = \lfloor \log_2 n \rfloor$ em qualquer caso.

21. a) $\sum_{k=1}^{0}[k(k+1)(k+2)] = 0 \times 1 \times 2 = 0 = (0 \times 1 \times 2 \times 3)/4$. Seja $n \geq 1$. Suponha, cmo hipótese de indução, que $\sum_{k=1}^{n}[k(k+1)(k+2)] = n(n+1)(n+2)(n+3)/4$. Tem-se: $\sum_{k=1}^{n+1}[k(k+1)(k+2)] = [\sum_{k=1}^{n}[k(k+1)(k+2)]] + (n+1)(n+2)(n+3)$. Aplicando-se a hipótese de indução, obtém-se que esta última é igual a $[n(n+1)(n+2)(n+3)/4] + (n+1)(n+2)(n+3)$. Simplificando-se esta, chega-se a $\sum_{k=1}^{n+1}[k(k+1)(k+2)] = (n+1)(n+2)(n+3)(n+4)/4$, o que completa a prova.

b) Inicialmente, veja que $3^0 - 7^0 - 2 = 0$, que é divisível por 8. Seja n um número natural arbitrário. Suponha como hipótese de indução que $3^n + 7^n - 2$ é divisível por 8. Tem-se: $3^{n+1} + 7^{n+1} - 2 = 3 \times 3^n + 7 \times 7^n - 2 = 3(3^n + 7^n - 2) + (4 \times 7^n + 4)$. Pela hipótese de indução, o primeiro termo desta última é divisível por 8. Assim, basta mostrar que o segundo, $4 \times 7^n + 4$ também é divisível por 8, o que será feito também por indução. Para $n = 0$: $4 \times 7^0 + 4 = 8$, que é divisível por 8. Seja $n \geq 0$, e suponha que $4 \times 7^n + 4$ é divisível por 8. Segue-se que $4 \times 7^{n+1} + 4 = 7(4 \times 7^n + 4) - 24$. O primeiro termo desta última é divisível por 8, pela hipótese de indução, e o segundo, 24, também é, o que leva à conclusão que $4 \times 7^{n+1} + 4$ é divisível por 8.

c) Tem-se: $\prod_{k=2}^{0}(1 - 1/k) = 1 - 1/2 = 1/2$. Seja $n \geq 2$, e suponha, como hipótese de indução, que $\prod_{k=2}^{n}(1 - 1/k) = 1/n$. Segue-se que: $\prod_{k=2}^{n+1}(1 - 1/k) = [\prod_{k=2}^{n}(1 - 1/k)] \times [1 - 1/(n+1)] = (1/n) \times [1 - 1/(n+1)]$, pela hipótese de indução. Esta última é igual a $(1/n) \times (n + 1 - 1)/(n+1)] = 1/(n+1)$, o que completa a prova.

d) $\sum_{k=1}^{2}(1/\sqrt{k}) = 1 + 1/\sqrt{2} = (\sqrt{2}+1)/\sqrt{2} = \sqrt{2}(\sqrt{2}+1)/2 > \sqrt{2}$, pois $\sqrt{2}+1 > 2$. Seja $n \geq 2$. Hipótese de indução: $\sum_{k=1}^{n}(1/\sqrt{k}) > \sqrt{n}$. Segue-se que: $\sum_{k=1}^{n+1}(1/\sqrt{k}) = [\sum_{k=1}^{n}(1/\sqrt{k})] + 1/\sqrt{n+1}$. Segue-se, pela hipótese de indução, que $\sum_{k=1}^{n+1}(1/\sqrt{k}) > \sqrt{n} + 1/\sqrt{n+1}$. Mas esta última é igual a $[\sqrt{n}\sqrt{n+1}+1]/\sqrt{n+1}$, que, por sua vez é igual a $\sqrt{n+1}[\sqrt{n}\sqrt{n+1}+1]/(n+1)$. Mas esta é maior do que $\sqrt{n+1}$, como requerido para completar a prova, pois $\sqrt{n}\sqrt{n+1}+1 > n+1$, já que $\sqrt{n}\sqrt{n+1} > n$.

22. Representando cada pessoa por um vértice e cada relacionamento de amizade por uma aresta, de tal forma que v, v' é uma aresta se, e somente se, as pessoas representadas por v e v' são amigas, deve-se mostrar que o grafo tem 2 vértices com o mesmo grau. Para

isto, pode-se usar o princípio do pombal, segundo o qual para se acomodar n pombos em menos de n casinhas, alguma casinha deverá receber mais de 1 pombo. Seja um grafo de n vértices, representando um grupo de n pessoas. Observando-se que um vértice pode ter de 0 a $n-1$ vértices adjacentes (o grafo não pode conter *loops* nem arestas múltiplas), considera-se 2 casos. Supondo que um certo vértice tem grau 0, então cada vértice só pode ter graus de 0 a $n-2$ (um vértice não pode ser adjacente a si mesmo nem àquele de grau 0). Por outro lado, se nenhum vértice tem grau 0, cada vértice só pode ter graus de 1 a $n-1$. Nos dois casos, pelo princípio do pombal, existem dois vértices com o mesmo grau.

23. Se cada vértice pode ter qualquer número de filhos, a altura é 0, se a árvore contém apenas 1 vértice, e é 2, se ela contém mais de 1 vértice; neste último caso, todos os vértices, com excessão da raiz, são filhos da raiz. Se cada vértice pode ter no máximo r filhos, a altura mínima é a de uma árvore que em cada nível k tem r^k vértices, com excessão, possivelmente, do último. Assim, a altura mínima, neste caso, é $\lfloor \log_r n \rfloor$, onde n é o número de vértices.

24. a) Uma árvore estritamente n-ária com i vértices internos tem $n \times i + 1$ vértices, já que cada um dos i vértice internos tem n filhos; e o termo 1 refere-se à raiz.
    b) Dado o resultado anterior, tem-se que uma árvore estritamente n-ária de k vértices tem $(k-1)/n$ vértices internos. Já o número de folhas é $k - i = k - (k-1)/n$.
    c) Uma árvore estritamente n-ária com k vértices tem altura mínima igual a $\lfloor \log_n k \rfloor$, e altura máxima igual a $\lceil (k-1)/n \rceil$.

25. $L = X$, onde $X = \{\mathtt{0}^m\mathtt{1}^n \mid m, n \geq 0\}$.

    $L \subseteq X$.

    Será provado por indução sobre o tamanho das palavras w que se $w \in L$ emtão $w \in X$. $\lambda = \lambda\lambda = \mathtt{0}^0\mathtt{1}^0 \in X$. Seja $n \geq 0$, e suponha, como hipótese de indução, que $x \in X$ se $x \in L$, para x tal que $|x| = n$. Para $w \in L$ tal que $|w| = n+1$ tem-se, pela definição de L, que $w = \mathtt{0}y$ ou $w = x\mathtt{1}$, onde x e y são palavras de L. Pela hipótese de indução, segue-se que $x \in X$ e $y \in X$, ou seja, ambos, x e y são da forma $\mathtt{0}^m\mathtt{1}^n$. Então $w = \mathtt{0}\mathtt{0}^m\mathtt{1}^n \in X$ ou $w = \mathtt{0}^m\mathtt{1}^n\mathtt{1} \in X$.

    $X \subseteq L$.

    Será provado por indução sobre o tamanho das palavras w que se $w \in X$ emtão $w \in L$. $\mathtt{0}^0\mathtt{1}^0 = \lambda\lambda = \lambda \in L$. Seja $n \geq 0$, e suponha, como hipótese de indução, que $x \in L$ se $x \in X$, para x tal que $|x| = n$. Para $w \in X$ tal que $|w| = n+1$ tem-se, que w é da forma $\mathtt{0}\mathtt{0}^m\mathtt{1}^n$ ou da forma $\mathtt{1}\mathtt{1}^n$, onde $m, n \geq 0$. No primeiro caso, pela hipótese de indução, segue-se que $\mathtt{0}^m\mathtt{1}^n \in L$; então, pela definição de L, $w \in L$. No segundo caso, como $\mathtt{1}\mathtt{1}^n = \mathtt{1}^n\mathtt{1}$, e, pela hipótese de indução, $\mathtt{1}^n \in L$, tem-se também que, pela definição de L, $w \in L$.

26. a) Definição recursiva de $L_1 = \{w \in \{\mathtt{0}, \mathtt{1}\} \mid |w| \text{ é par}\}$:
        - $\lambda \in L_1$;
        - se $y \in L_1$, então $\mathtt{00}y, \mathtt{01}y, \mathtt{10}y, \mathtt{11}y \in L_1$.
    b) Definição recursiva de $L_2 = \{w \in \{\mathtt{0}, \mathtt{1}\} \mid w \text{ é palíndromo}\}$:
        - $\lambda, \mathtt{0}, \mathtt{1} \in L_2$;
        - se $w \in L_2$, então $\mathtt{0}w\mathtt{0}, \mathtt{1}w\mathtt{1} \in L_2$.
    c) Definição recursiva de $L_3 = \{w \in \{\mathtt{0}, \mathtt{1}\} \mid w \text{ contém } \mathtt{00}\}$:

- $\mathtt{00} \in L_3$;
- se $w \in L_3$, então $\mathtt{0}w, \mathtt{1}w, w\mathtt{0}, w\mathtt{1} \in L_3$.

d) Definição recursiva de $L_4 = \{w \in \{\mathtt{0}, \mathtt{1}\} \mid w$ não contém $\mathtt{00}\}$:

- $\lambda, \mathtt{0} \in L_4$;
- se $y \in L_4$, então $y\mathtt{1}, y\mathtt{10} \in L_4$.

e) Definição recursiva de $L_5 = \{\mathtt{0}^{n^2} \mid n \in \mathbf{N}\}$:

- $\lambda \in L_5$;
- se $y \in L_5$, então $y\mathtt{0}^{2\sqrt{|y|}+1} \in L_5$.

f) Definição recursiva de $L_6 = \{w \mid w$ é uma permutação dos dígitos 1, 2 e 3$\}$:

- $123 \in L_6$;
- se $abc \in L_6$, então $acb \in L_6$ e $bca \in L_6$, onde $a, b, c \in \{1, 2, 3\}$.

g) Definição recursiva de $L_7 = \{w \mid w$ é uma permutação dos 10 dígitos decimais$\}$:

- $\mathtt{0123456789} \in L_7$;
- se $xab \in L_7$ ou $axb \in L_7$, então $xba \in L_7$, onde $a, b \in \{\mathtt{1}, \mathtt{2}\}$ e $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^*$.

27. Definição recursiva de *concatenação*:

- $x\lambda = x$ para $x \in \Sigma^*$;
- se $x(ya) = (xy)a$ para $x, y \in \Sigma^*$ e $a \in \Sigma$.

Será provado que $(xy)z = x(yz)$ por indução sobre $|z|$. Para $z = \lambda$, tem-se: $(xy)\lambda = xy = x(y\lambda)$. Seja $n \geq 0$. Suponha que $(xy)z = x(yz)$ para toda palavra z tal que $|z| = n$. Seja w uma palavra de $n+1$ símbolos. Então $w = za$ para uma palavra z de n símbolos e $a \in \Sigma$. Segue-se que $(xy)w = (xy)(za) = ((xy)z)a$, pela definição de concatenação. Prosseguindo: $((xy)z)a = (x(yz))a$, pela hipótese de indução. E, aplicando-se duas vezes a definição de concatenação, determina-se que $(x(yz))a = x((yz)a) = x(y(za))$, o que conclui a argumentação, visto que $x(y(za)) = x(yw)$.

Definição recursiva de *reverso*:

- $\lambda^R = \lambda$;
- se $x^R = y$ e $a \in \Sigma$ então $(xa)^R = ax^R$.

Será provado que $(xy)^R = y^R x^R$ por indução sobre $|y|$. Para $y = \lambda$, tem-se: $(xy)^R = (x\lambda)^R = x^R = \lambda x^R = \lambda^R x^R = y^R x^R$. Seja $n \geq 0$, e suponha que $(xy)^R = y^R x^R$ para palavras y tal que $|y| = n$. Seja w uma palavra de $n+1$ símbolos, ou seja $w = za$ para uma palavra z de n símbolos e $a \in \Sigma$. Então $(xw)^R = (x(za))^R = ((xz)a)^R$, pela definição de concatenação. E $((xz)a)^R = a(xz)^R$, pelas definição de reverso. Pela hipótese de indução, segue-se que $a(xz)^R = a(z^R x^R)$. Pelo resultado acima (associatividade da concatenação), $a(z^R x^R) = (az^R)x^R$, e pela definição de reverso, $(az^R)x^R = (za)^R x^R = w^R x^R$.

A seguir, mostra que se w é palíndromo, $w = vv^R$ ou $w = vav^R$ para algum $v \in \Sigma^*$ e $a \in \Sigma$. Seja w um palíndromo. Se $|w|$ é par, então $w = xy$, onde $|x| = |y| \geq 0$. Como w é palíndromo, $w = xy = (xy)^R = y^R x^R$. De $xy = y^R x^R$ e do fato de que $|x| = |y| = |y^R|$, segue-se que $y^R = x$ (e $x^R = y$). Assim, $w = xy = xx^R$. Agora, suponha que $|w|$ é ímpar. Então $w = xay$, onde $|x| = |y| \geq 0$, $a \in \Sigma$. Como w é palíndromo, $w = xay = (xay)^R = y^R(xa)^R = y^R ax^R$. Como $w = xay = y^R ax^R$ e $|x| = |y| = |y^R|$, segue-se que $y^R = x$ (e $x^R = y$) e, portanto, $w = xay = xax^R$.

28. De $x = x^R$, $y = y^R$ e $xy = (xy)^R = y^R x^R$, deduz-se que $xy = yx$. Será mostrado por indução forte sobre $|xy|$ que, neste caso, existem $k, n \in \mathbf{N}$ e z tais que $x = z^k$ e $y = z^n$. Seja $m \geq 0$ e suponha, como hipótese de indução, que o resultado valha para todo x e y tais que $|xy| < m$. Sejam, então duas palavras quaisquer x e y tais que $|xy| = m$. Se $m = 0$, $x = y = \lambda$, e basta fazer $k = n = 0$. Seja, então, x e y tais que $|xy| \geq 1$. São 3 casos a considerar: $|x| = |y|$, $|x| < |y|$ e $|x| > |y|$. No primeiro caso, tem-se que $x = y$ e, portanto, basta fazer $z = x$ e $k = n = 1$. No segundo caso, deve existir uma palavra s tal que $y = xs$. Como $xy = yx$, segue-se que $xxs = xsx$, que implica que $xs = sx$. Desta última, pela hipótese de indução, existem u, i e j tais que $x = u^i$ e $s = u^j$. Assim, $y = xs = u^{i+j}$. Isto mostra que o resultado vale tomando-se $z = u$, $k = i$ e $n = i + j$. O terceiro caso é similar a este último.

29. Seja $X \subseteq L^*$. Por indução sobre o tamanho de uma palavra w, será mostrado que $w \in L^*$ se, e somente se, $w \in (L^* \cup X)^*$. Tem-se: $\lambda \in (L^* \cup X)^*$ e $\lambda \in L^*$, por definição. Seja uma palavra w tal que $|w| > 0$. Se $w \in L^*$, então, por definição, $w = xy$, onde $x \in L^*$ e $y \in L$. Como $x \in L^*$, $x \in L^* \cup X$ e também $x \in (L^* \cup X)^*$. Como $y \in L$, $y \in L^*$ e também $y \in L^* \cup X$. Logo $xy = w \in (L^* \cup X)^*$. Por outro lado, se $w \in (L^* \cup X)^*$, $w = xy$, onde $x \in (L^* \cup X)^*$ e $y \in L^* \cup X$. Como $X \subseteq L^*$, $y \in L^*$. Pela hipótese de indução, $x \in L^*$. Assim, segue-se que $xy = w \in L^*$.

30. Como Σ_1 e Σ_2 são alfabetos, Σ_1^* e Σ_2^* são enumeráveis. Assim, sejam $f_1 : \Sigma_1^* \to \mathbf{N}$ e $f_2 : \Sigma_2^* \to \mathbf{N}$ funções bijetoras. A função $g : \Sigma_1^*\Sigma_2^* \to \mathbf{N}$, onde $g(xy) = (f_1(x) + f_2(y))(f_1(x) + f_2(y) + 1)/2 + f_1(x)$ para $x \in \Sigma_1^*$ e $y \in \Sigma_2^*$, é bijetora. Logo, $\Sigma_1^*\Sigma_2^*$ é enumerável.

31. Por indução sobre n. O domínio de $H_0 : \Sigma^0 \times \Sigma^0 \to \mathbf{N}$ é $\{(\lambda, \lambda)\}$, e tem-se que $H_0(\lambda, \lambda) = 0$, e portanto $H_0(\lambda, \lambda) = H_0(\lambda, \lambda) + H_0(\lambda, \lambda)$. Seja $n \geq 0$ e suponha, como hipótese de indução, que $H_n(x, y) \leq H_n(x, z) + H_n(z, y)$ para qualquer palavra z de Σ^n. Sejam $a, b, c \in \Sigma$. Será mostrado que $H_{n+1}(xa, yb) \leq H_n(xa, zc) + H_n(zc, yb)$. Considera-se 5 casos:

    $a = b = c$.
    Então $H_{n+1}(xa, yb) = H_n(x, y)$, $H_{n+1}(xa, zc) = H_n(x, z)$ e $H_{n+1}(zc, yb) = H_n(z, y)$. Como, pela hipótese de indução, $H_n(x, y) \leq H_n(x, z) + H_n(z, y)$, $H_{n+1}(xa, yb) \leq H_n(xa, zc) + H_n(zc, yb)$.

    $a = b \neq c$.
    Então $H_{n+1}(xa, yb) = H_n(x, y)$, $H_{n+1}(xa, zc) = H_n(x, z) + 1$ e $H_{n+1}(zc, yb) = H_n(z, y) + 1$. Como, pela hipótese de indução, $H_n(x, y) \leq H_n(x, z) + H_n(z, y)$, segue-se que $H_n(x, y) < H_n(x, z) + 1 + H_n(z, y) + 1$ e, portanto, $H_{n+1}(xa, yb) < H_n(xa, zc) + H_n(zc, yb)$.

    $a = c \neq b$.
    Então $H_{n+1}(xa, yb) = H_n(x, y) + 1$, $H_{n+1}(xa, zc) = H_n(x, z)$ e $H_{n+1}(zc, yb) = H_n(z, y) + 1$. Como, pela hipótese de indução, $H_n(x, y) \leq H_n(x, z) + H_n(z, y)$, segue-se que $H_n(x, y) + 1 \leq H_n(x, z) + H_n(z, y) + 1$ e, portanto, $H_{n+1}(xa, yb) \leq H_n(xa, zc) + H_n(zc, yb)$.

    $b = c \neq a$.
    Então $H_{n+1}(xa, yb) = H_n(x, y) + 1$, $H_{n+1}(xa, zc) = H_n(x, z) + 1$ e $H_{n+1}(zc, yb) = H_n(z, y)$. Como, pela hipótese de indução, $H_n(x, y) \leq H_n(x, z) + H_n(z, y)$, segue-se que $H_n(x, y) + 1 \leq H_n(x, z) + 1 + H_n(z, y)$ e, portanto, $H_{n+1}(xa, yb) \leq H_n(xa, zc) + H_n(zc, yb)$.

    $a \neq b \neq c$.
    Então $H_{n+1}(xa, yb) = H_n(x, y) + 1$, $H_{n+1}(xa, zc) = H_n(x, z) + 1$ e $H_{n+1}(zc, yb) =$

$H_n(z,y)+1$. Como, pela hipótese de indução, $H_n(x,y) \leq H_n(x,z) + H_n(z,y)$, segue-se que $H_n(x,y)+1 < H_n(x,z)+1+H_n(z,y)+1$ e, portanto, $H_{n+1}(xa,yb) < H_n(xa,zc)+H_n(zc,yb)$.

Assim, vê-se que, em qualquer caso, $H_{n+1}(xa,yb) \leq H_n(xa,zc) + H_n(zc,yb)$.

32. a) Gramática para $\{w \in \{\mathtt{0},\mathtt{1}\}^* \mid w \text{ não contém } \mathtt{00}\}$:

$$\begin{aligned} P &\to \mathtt{0}A \mid \mathtt{1}P \mid \lambda \\ A &\to \mathtt{1}P \mid \lambda \end{aligned}$$

b) Gramática para $\{\mathtt{0}^n\mathtt{1}^{2n+1}\mathtt{0}^n \mid n \in \mathbf{N}\}$:

$$\begin{aligned} P &\to \mathtt{0}UP\mathtt{0} \mid \mathtt{1} \\ U\mathtt{1} &\to \mathtt{111} \\ U\mathtt{0} &\to \mathtt{0}U \end{aligned}$$

c) Gramática para $\{w\mathtt{0}w \mid w \in \{\mathtt{1},\mathtt{2}\}^*\}$:

$$\begin{aligned} P &\to \mathtt{1}PU \mid \mathtt{2}PD \mid \mathtt{0} \\ \mathtt{0}U &\to \mathtt{01} \\ \mathtt{0}D &\to \mathtt{02} \\ \mathtt{1}U &\to U\mathtt{1} \\ \mathtt{2}U &\to U\mathtt{2} \\ \mathtt{1}D &\to D\mathtt{1} \\ \mathtt{2}D &\to D\mathtt{2} \end{aligned}$$

d) Gramática para $\{\mathtt{a}^n\mathtt{b}^n\mathtt{c}^k \mid 0 \leq n < k\}$:

$$\begin{aligned} P &\to AS \\ A &\to \mathtt{a}A\mathtt{b}C \mid \lambda \\ C\mathtt{b} &\to \mathtt{b}C \\ C\mathtt{c} &\to \mathtt{cc} \\ S &\to \mathtt{c}S \mid \mathtt{c} \end{aligned}$$