

# Teoria da Computação

## Técnicas de Demonstração

Simão Melo de Sousa

12 de Outubro de 2011

### Conteúdo

1	Conjuntos	1
2	Demonstração Por Contradição	2
3	Princípios da gaiola de pombos	3
4	Indução Estrutural	5
5	Indução Bem Fundada	16
6	Técnica da Diagonal	20

## 1 Conjuntos

**Exercício 1** *Demonstre que o conjunto dos inteiros  $\mathbb{Z}$  é numerável.*

**Resposta**  $\square$

**Exercício 2** *Demonstre que o produto cartesiano  $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$  de dois conjuntos  $X$  e  $Y$  numeráveis é numerável.*

**Resposta**  $\square$

## 2 Demonstração Por Contradição

**Exercício 3** *Demonstre por contradição o teorema seguinte provado originalmente por Euclides.*

Existe uma infinidade de números primos

**Resposta**  $\square$

**Exercício 4** *Demonstre, por contradição, que  $2 - \sqrt{2}$  não é racional. Estude por exemplo as contribuições da expressão  $(2 - \sqrt{2})^2$  ao raciocínio por contradição pedido.*

**Resposta**  $\square$

**Exercício 5** *Assuma a existência das seguintes variáveis proposicionais  $P$  e  $Q$ . Usando o princípio da redução ao absurdo, demonstre que*

1. (Terço excluído)  $P \vee \neg Q$

**Resposta**

2. (Lei de Pierce)  $((P \implies Q) \implies P) \implies P$

**Resposta**

3. (Uma das leis de De Morgan)  $\neg(\neg P \wedge \neg Q) \implies (P \vee Q)$

**Resposta**

$\square$

**Exercício 6** *Demonstre por contradição o teorema seguinte: Não existe  $x, y \in \mathbb{N} \wedge x > 0 \wedge y > 0$  tal que  $x^2 - y^2 = 1$*

**Resposta**  $\square$

**Exercício 7** *Demonstre por contradição que não existe  $n \in \mathbb{N} \wedge n \leq 0$  tal que  $2n^9 + 5n^7 - 6n^4 - n^2 - 27 = 0$ .*

**Resposta**  $\square$

**Exercício 8** *Demonstre por contradição que não existe raiz racional para a equação  $x^3 + x + 1 = 0$ .*

**Resposta**  $\square$

**Exercício 9** *Numa ilha longe, cada habitante ou diz sempre a verdade ou mente compulsivamente. O João e a Maria moram nesta ilha.*

João diz: "Exactamente um de nós está a mentir"

*A Maria acrescenta: "O João diz a verdade"  
Diga quem mente e quem diz verdade.*

**Resposta**  $\square$

**Exercício 10** *Assuma a existência da prova do teorema de pitágoras para este exercício. Demonstre por contradição o seguinte enunciado, conhecido por "inversa do teorema de Pitágoras".*

Considere um triângulo de lados não nulos  $a$ ,  $b$  e  $c$  tal que  $a^2 + b^2 = c^2$ . Então o triângulo é rectângulo.

**Resposta**  $\square$

**Exercício 11** *Demonstre por contradição os seguintes enunciados:*

1.  $\sqrt[3]{2}$  é irracional.

**Resposta**

2. Não há inteiros naturais não nulos solução para a equação  $x^2 - y^2 = 10$ .

**Resposta**

3. Não há número racional solução da equação  $x^5 + x^4 + x^3 + x^2 + 1 = 0$ .

**Resposta**

4. Se  $a$  é um número racional e  $b$  um número irracional então  $a + b$  é irracional.

**Resposta**

$\square$

### 3 Princípios da gaiola de pombos

**Exercício 12**

- *Demonstre, utilizando o princípios da gaiola de pombos, que se se escolher 7 números distintos de  $\{1, 2, \dots, 11\}$  então dois dos números escolhidos tem uma soma de 12.*

**Resposta**

- *Generalize o resultado anterior:*

– *Demonstre que se seleccionar  $n + 1$  números no intervalo inteiro  $\{1, 2, \dots, 2n - 1\}$  então necessariamente existe dois desses inteiros cuja soma é  $2n$ .* **Resposta**

– *Mostre que é possível seleccionar  $n$  números deste intervalo sem que exista dois inteiros da selecção cuja soma é  $2n$ .* **Resposta**

– *Formule e prove uma propriedade semelhante para o intervalo  $\{1, 2, \dots, 2n\}$ .* **Resposta**

□

**Exercício 13** *Considere o seguinte enunciado:*

*Sejam  $a_1 \dots a_n \in \mathbb{N}$ ,  $n$  inteiros naturais positivos distintos. Então existe sempre 2 destes valores cuja a diferença é divisível por  $n - 1$ .*

*Utilize o princípio da gaiola de pombos para demonstra-lo.*

**Resposta** □

**Exercício 14**

• *Demonstre que se 5 pontos são seleccionados no interior de um quadrado de dimensão  $1 \times 1$  então existe dois pontos cuja a distância que os separa é menor do que  $\frac{\sqrt{2}}{2}$ .*

**Resposta**

• *Demonstre que se 4 pontos forem seleccionados no interior de um círculo unitário então existe necessariamente dois pontos cuja a distância de separação seja menor do que  $\sqrt{2}$ .*

**Resposta**

• *Quantos pontos devem ser seleccionados no interior de um triângulo equilátero para garantir que dois destes pontos tem uma distância de separação menor do que 1?*

**Resposta**

□

**Exercício 15** Para um subconjunto  $X \subseteq \{1, 2, \dots, 9\}$ , define-se uma função  $\sigma(X) = \sum_{x \in X} x$  (Por exemplo  $\sigma(\{1, 6, 8\}) = 1 + 6 + 8 = 15$ ). Demonstre que dos 26 subconjuntos de  $\{1, 2, \dots, 9\}$  de tamanho menor ou igual a 3, há subconjuntos  $A$  e  $B$  tais que  $\sigma(A) = \sigma(B)$ .

**Resposta** □

**Exercício 16** Pedro é atleta de alto nível de triathlon e está a planear o período de treino que durará 44 dias. Pedro pretende treinar pelo menos uma vez por dia e no total 70 vezes. demonstre que então terá um período de  $n$  dias consecutivos que terá de treinar no total exactamente 17 vezes (i.e. número de treinos no total destes  $n$  dias é 17).

**Resposta** □

**Exercício 17** O Paquito Venâncio pretende organizar uma festa para  $n$  pessoas ( $n \geq 2$ , para ter a certeza que não fica sozinho). Assumindo que se  $x$  é amigo de  $y$  então  $y$  é amigo de  $x$ , demonstre então que qualquer que seja as  $n$  pessoas convidadas, existe sempre duas dessas pessoas com exactamente o mesmo número de amigos.

**Resposta** □

**Exercício 18** 6 pessoas se juntaram num jantar. Ou 3 delas se conheciam mutuamente antes do jantar ou 3 delas se desconheciam completamente antes do jantar.

**Resposta** □

**Exercício 19** Considere uma cidade dividida em dois bairros. Nesta cidade há 10000 linhas telefónicas diferentes. O números de telefone desta cidade tem 4 dígitos e mais de metade destas linhas estão no primeiro dos dois bairros. Então existe dois números de telefone no primeiro bairro tal que a soma é um número de telefone que pertence igualmente ao bairro.

**Resposta** □

## 4 Indução Estrutural

**Exercício 20** Demonstre por indução estrutural que:

- $\forall n \in \mathbb{N}. (3^{3 \cdot n + 2} + 2^{n+4})$  é divisível por 5.

**Resposta**

- $\forall n \in \mathbb{N}^*, 1.2.3 + 2.3.4 + \dots + n.(n+1).(n+2) = \frac{n.(n+1).(n+2).(n+3)}{4}$ . **Resposta**

- $n^4 - 4.n^2$  é divisível por 3 para todo o  $n \geq 0$ . **Resposta**

- $\sum_{k=0}^n k = \frac{n(n+1)}{2}$ . **Resposta**

- $\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}$ . **Resposta**

- $\sum_{k=0}^n k^3 = \frac{n^2(n+1)^2}{4}$ . **Resposta**

- $\sum_{k=0}^n (a.r)^k = \frac{a(1-r^{n+1})}{(1-r)}$ . **Resposta**

- $\forall n \in \mathbb{N}, n^2(n^2 - 1)$  é divisível por 12. **Resposta**

□

**Exercício 21** Demonstre por indução estrutural sobre  $n$  que  $\forall n \in \mathbb{N}, n^2(n^2 - 1)$  é divisível por 12. □

**Exercício 22** Vamos aqui considerar o conjunto  $\mathbb{N}^*$  (os naturais sem o 0). Considere a seguinte sequência de somas:

$$\frac{1}{1 \times 2}; \quad \frac{1}{1 \times 2} + \frac{1}{2 \times 3}; \quad \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4}; \quad \dots$$

- Calcule as somas do exemplo e apresente um padrão geral para esta sequência de somas.
- Demonstre **por indução estrutural** a conjectura apresentada na alínea anterior.

□

**Exercício 23** Seja  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ , a função recursiva definida por:

$$f(m, n) \triangleq \begin{cases} n + 1 & \text{se } m = 0 \\ f(m - 1, 1) & \text{se } n = 0 \wedge m \neq 0 \\ f(m - 1, f(m, n - 1)) & \text{se } n > 0 \wedge m > 0 \end{cases}$$

Demonstre por indução que  $\forall k \in \mathbb{N}, f(1, k) = k + 2$

**Resposta**

demonstre por indução que  $\forall k \in \mathbb{N}, f(2, k) = 2 \times k + 3$ . □

**Exercício 24**

1. Defina de forma indutiva o conjunto  $\text{bin}_A$  das árvores binárias não vazias de elementos dum conjunto  $A$ . Por árvores não vazias, entendemos que as mais pequenas árvores deste conjunto são folhas (árvores com um só elemento do conjunto  $A$ );
2. Dê o princípio de indução associada a esta definição indutiva;
3. Defina a função arestas que calcula o número de vértice da árvore em parâmetro;
4. Defina a função nodos que calcula o número de nodos da árvore em parâmetro;
5. Demonstre que  $\forall a \in \text{bin}_A, \text{nodos}(a) = \text{arestas}(a) + 1$ .

**Resposta**

□

**Exercício 25** Explique brevemente a diferença entre a noção de função recursiva e a noção de função estruturalmente recursiva.

**Resposta**

□

**Exercício 26** Neste exercício vamos considerar uma definição indutiva das fórmulas da lógica proposicional.

Seja  $\mathcal{V} \triangleq \{P, Q, R, S, \dots\}$  um conjunto numerável de variáveis chamadas variáveis proposicionais. Seja  $\mathcal{C}$  o conjunto de conectivas  $\{\wedge, \vee, \rightarrow, \neg, \perp, \top\}$ .

O conjunto  $\mathcal{P}rop$  das fórmulas proposicionais é definido como o menor subconjunto  $X$  do monoíde livre  $(\mathcal{V} \cup \mathcal{C} \cup \{", "\})^*$  verificando os (B) e (I) seguintes:

- (B):
1. Para todo o  $x \in \mathcal{V}$ ,  $x$  pertence a  $X$
  2.  $\top$  pertence a  $X$
  3.  $\perp$  pertence a  $X$
- (I):
1. Seja  $F$  uma fórmula de  $X$  ( $F \in X$ ), então  $\neg F \in X$
  2. Sejam  $F$  e  $G$  duas fórmulas de  $X$  (i.e.  $F, G \in X$ ), então  $(F \wedge G) \in X$
  3. Sejam  $F$  e  $G$  duas fórmulas de  $X$ , então  $(F \vee G) \in X$
  4. Sejam  $F$  e  $G$  duas fórmulas de  $X$ , então  $(F \rightarrow G) \in X$
1. Dê o princípio de indução associada a esta definição indutiva;
  2. Seja  $npe : \mathcal{P}rop \rightarrow \mathbb{N}$ , a função que devolve o número de parêntesis esquerdos da fórmula em parâmetro. De forma semelhante, seja  $npd : \mathcal{P}rop \rightarrow \mathbb{N}$ , a função que devolve o número de parêntesis direitos da fórmula em parâmetro. Demonstre que  $\forall F \in \mathcal{P}rop, npe(F) = npd(F)$ .

**Resposta**

□

**Exercício 27** O objectivo deste exercício é a definição indutiva do conjunto das datas válidas. Uma data válida é um terno  $(d, m, a)$  onde  $d$  e  $a$  são inteiros que representam respectivamente o dia e o ano, e  $m$  uma palavra representando um mês (como a palavra “Fevereiro” que representa o mês de Fevereiro). Imagine que exista uma relação ternária  $val(d, m, a)$  que seja verdade se o dia  $d$  é um dia possível para o mês  $m$  e o ano  $a$ . Por exemplo não temos  $val(29, Fevereiro, 2001)$  porque 2001 não é um ano bissexto, também não temos  $val(31, Setembro, 2001)$  nem  $val(0, Setembro, 2001)$  porque Setembro só tem 30 dias e porque não existe o dia 0.

1. Defina indutivamente o conjunto Mês dos meses.



2. Defina indutivamente o conjunto Data das datas válidas.

□

**Exercício 28** Considere o tipo *expr* das expressões aritméticas simples seguintes:

```

1 (* tipo expr onde:
2   I = constante inteira, V = variável, A = +, S = -, M = *, D = /
3 *)
4 type expr = I of int | V of string | A of expr*expr
5             | S of expr*expr | M of expr*expr | D of expr*expr
6
7 (* tipo dos ambientes (associação variável-valor)*)
8 type env = (string*int) list

```

Considere igualmente a função *eval* seguinte:

```

1 let rec eval (e:expr) (ambiente: env)=
2   match e with
3     | I i → i
4     | V v → assoc v ambiente
5     | A (e1,e2) → eval e1 ambiente + eval e2 ambiente
6     | S (e1,e2) → eval e1 ambiente - eval e2 ambiente
7     | M (e1,e2) → eval e1 ambiente * eval e2 ambiente
8     | D (e1,e2) → eval e1 ambiente / eval e2 ambiente

```

onde *assoc* é a função que devolve o valor inteiro associado a parâmetro *v* no ambiente *ambiente*, se este existir.

- (2 minutos) Qual é o princípio de indução associada a definição indutiva de *expr*?

**Solução:**

►

de uma forma compacta:

$$\begin{aligned}
 & \forall i \in \mathbb{N} P(I\ i) \wedge \forall x \text{ variável}, P(V\ x) \wedge \\
 & (\forall e_1, e_2 \in \text{expr}, P(e_1) \wedge P(e_2) \Rightarrow P(A\ e_1\ e_2) \wedge P(S\ e_1\ e_2) \wedge P(M\ e_1\ e_2) \wedge P(D\ e_1\ e_2)) \\
 & \Rightarrow \forall e \in \text{expr}, P(e)
 \end{aligned}$$

ou seja se temos  $P(V\ x)$  e  $P(I\ i)$  para qualquer variável  $x$  e inteiro  $i$  e se para todos  $e_1$  e  $e_2$  expressões,  $P(e_1) \wedge P(e_2)$  implicam  $P(A\ e_1\ e_2)$ ,

$P(S\ e_1\ e_2)$ ,  $P(M\ e_1\ e_2)$  e  $P(D\ e_1\ e_2)$  então  $P$  é válido para todo o elemento de  $expr$  (ou seja  $\forall e \in expr, P(e)$ )



- (15 minutos) Defina uma função *simplify* :  $expr \rightarrow expr$  que execute sobre toda a estrutura do seu parâmetro as transformações seguintes:

$$\begin{aligned} e + 0 = e & & e - 0 = e \\ \text{para uma qualquer expressão } e, & & e * 1 = e & & e / 1 = e \\ & & e + e = 2 * e & & e - e = 0 \end{aligned}$$

Por exemplo a expressão  $\frac{(x+0)+x}{1}$  se simplifica em  $2 * x$  porque, pelas regras definidas,  $\frac{(x+0)+x}{1}$  se transforma em  $((x + 0) + x)$ ,  $x + 0$  se transforma em  $x$  e  $x + x$  se transforma em  $2 * x$ . Repare que a ordem de aplicação destas simplificações é irrelevante se todas elas são de facto executadas.

### Solução:



```

1
2 let rec simplify e =
3   match e with
4     | I i → I i
5     | V v → V v
6     | A (e1,e2) → let e'1,e'2 = simplify e1, simplify e2 in
7       if e'1 = I 0 then e'2
8       else if e'2 = I 0 then e'1
9       else if e'1=e'2
10          then if e'1 = I 1 then I 2 (* uma pequena optimização não re
11             else (M(I 2,e'1)))
12          else A(e'1,e'2)
13     | S (e1,e2) → let e'1,e'2 = simplify e1, simplify e2 in
14       if e'2 = I 0 then e'1
15       else if e'1 = e'2 then I 0 else S(e'1,e'2)
16     | M (e1,e2) → let e'1,e'2 = simplify e1, simplify e2 in
17       if e'1= I 1 then e'2
18       else if e'2 = I 1 then e'1
19       else if (e'1 = I 0) || (e'2 = I 0) then I 0 (*não exigido....*)

```

```

20     else M(e'1,e'2)
21   / D (e1,e2) → let e'1,e'2 = simplify e1, simplify e2 in
22     if e'2= I 1 then e'1
23     else if e'1 = e'2 then (I 1) (*não exigido...*)
24     else if e'2 = I 0 then failwith "divisão por zero" (*não exigido...*)
25     else D (e'1,e'2)

```



- (15 minutos) Demonstre por indução que  $\forall e : \text{expr}, \forall a : \text{env}, \text{eval}(\text{simplify } e) a = \text{eval } e a$ . Assuma para esse efeito e se necessário que o ambiente  $a$  tem todas as propriedades desejadas. Por exemplo, o ambiente tem todas as variáveis presentes na expressão considerada.

### Solução:



Provemos esta enunciado por indução sobre a estrutura do parâmetro  $e$ .

- Casos de base. Consideremos um inteiro  $i$  e uma variável  $x$ . É trivial verificar que por definição de `simplify`,  $\text{eval}(\text{simplify } (V x)) = \text{eval}(V x)$  e  $\text{eval}(\text{simplify } (I i)) = \text{eval}(I i)$ .
- Passo indutivo. Em moldes gerais, as operações e simplificações operadas não alteram o resultado. É esse facto que vamos verificar. Vamos somente resolver o caso da soma, sendo os outros casos muito semelhantes (fica em exercício). Consideremos então  $e_1$  e  $e_2$  duas expressões.

Hipótese de Indução:  $\text{eval}(\text{simplify } e_1) = \text{eval } e_1$  e  $\text{eval}(\text{simplify } e_2) = \text{eval } e_2$ .

Objectivo: provar que sob estas hipóteses temos necessariamente  $\text{eval}(\text{simplify } (A e_1 e_2)) = \text{eval } (A e_1 e_2)$ .

A parte do código que nos interessa aqui é:

```

1     (...)
2   / A (e1,e2) → let e'1,e'2 = simplify e1, simplify e2 in
3     if e'1 = I 0 then e'2
4     else if e'2 = I 0 then e'1
5     else

```

```

6         if e'1=e'2 then
7             if e'1 = I 1 then I 2
8             else (M(I 2, e'1))
9         else A(e'1, e'2)

```

- \* Temos  $\text{simplify } e_1 = e'_1$  e  $\text{simplify } e_2 = e'_2$ . Assim, pelas hipóteses de indução, sabemos que  $\text{eval } e_1 = \text{eval } (\text{simplify } e_1) = \text{eval } e'_1$  e que  $\text{eval } e_2 = \text{eval } (\text{simplify } e_2) = \text{eval } e'_2$ .
- \* Por consequência  $\text{eval}(A e_1 e_2) = \text{eval } e_1 + \text{eval } e_2 = \text{eval } e'_1 + \text{eval } e'_2$ . Resta agora saber se é igual a  $\text{eval } (\text{simplify } (A e_1 e_2))$ .
- \* De facto o resultado de  $(\text{simplify } (A e_1 e_2))$  depende da forma de  $e'_1$  e de  $e'_2$ .
  - Se  $e'_1 = I 0$  então, por definição de  $\text{simplify}$ ,  $(\text{simplify } (A e_1 e_2)) = e'_2$ . Ora acontece que se  $e'_1 = I 0$  então  $\text{eval } e'_1 = I 0 = \text{eval } e_1$ , por consequência  $\text{eval}(A e_1 e_2) = \text{eval } e_2 = \text{eval } e'_2 = \text{eval } (\text{simplify } (A e_1 e_2))$ . Caso resolvido.
  - Caso  $e'_2 = I 0$ . Idêntico ao caso anterior.
  - Caso  $e'_1 = e'_2$ . Neste caso  $\text{eval } e'_1 = \text{eval } e'_2$  e  $\text{eval}(A e_1 e_2) = \text{eval } e'_1 + \text{eval } e'_2 = 2 \times \text{eval } e'_1$ . que coincide com o resultado de  $\text{eval } (\text{simplify } (A e_1 e_2))$ . No caso de  $\text{eval } e'_1 = I 1$  esta propriedade mantém-se. Caso resolvido.
  - No caso geral (nenhum destes casos particulares ocorrem),  $\text{eval } (\text{simplify } (A e_1 e_2)) = \text{eval } (A e'_1 e'_2) = \text{eval } e'_1 + \text{eval } e'_2 = \text{eval } (A e_1 e_2)$ . Caso resolvido.

QED.



□

**Exercício 29** Definir os seguintes conjuntos indutivos:

1. A parte  $\mathbb{N}_3$  de  $\mathbb{N}$  dos inteiros múltiplos de três.
2. A parte  $L_A$  do monoide livre  $B^*$  (onde o alfabeto  $B$  é  $A \cup \{ '[', ']', ':', ']' \}$ ) das listas de elementos de um conjunto  $A$ . Fornecer igualmente a definição constructiva do conjunto considerado.

3. A parte  $AB_A$  do monoide livre  $B^*$  (onde o alfabeto  $B$  é  $A \cup \{(')', '!', '\}'\}$ ) das árvores de elementos de um conjunto  $A$ .
4. A parte  $D$  do monoide livre  $A^*$  (onde o alfabeto  $A$  é  $\{(\,)\}$ ) das expressões bem "parentesadas" (conhecida por Linguagem de Dyck. Por exemplo  $()(())$ ,  $()()$  e  $((()))$  são palavras da linguagens de Dyck, mas  $((), ())$  e  $()()$  não são palavras da linguagem.
5. A parte  $A^*$  do monoide livre  $A^*$  (sendo  $A$  um alfabeto qualquer).

□

**Exercício 30** Seja  $A$  um alfabeto, define-se  $AB_{A,n}$ , ( $n \in \mathbb{N}$ ) por

$$AB_{A,0} = \{\emptyset\} \tag{1}$$

$$AB_{A,n+1} = AB_{A,n} \cup \{(a, g, d) \mid a \in A \text{ e } g, d \in AB_{A,n}\} \tag{2}$$

1. Mostrar que  $AB_{A,\omega} (= \bigcup_{n \in \mathbb{N}} AB_{A,n})$  é o conjunto  $AB_A$ .
2. Para  $A = \{a, b, c\}$ , exibir  $AB_{A,2}$ .
3. Exibir uma árvore binária que não pertença a  $AB_A$ . Porque nunca será ela gerado por  $AB_{A,\omega}$ ?

□

**Exercício 31** Explique brevemente a importância da noção de não ambiguidade aquando da definição de funções por recursividade estrutural

**Resposta** □

**Exercício 32** Qual é a altura de 18 nos conjuntos indutivo dos inteiros, dos inteiros pares, dos inteiros múltiplos de três?

□

**Exercício 33** Seja o polinómio  $p(x) = \frac{1}{3}x^3 - \frac{1}{2}x^2 + \frac{1}{6}x$

1. Definir  $p(x+1) - p(x)$ .
2. Mostrar que para todo o  $n \in \mathbb{N}$ ,  $p(x) \in \mathbb{N}$ .

□

**Exercício 34** *Mostrar que qualquer palavra da linguagem de Dyck tem tantas parêntesis esquerdas como parêntesis direitas.*

□

**Exercício 35** *Encontrar o erro no raciocínio seguinte:*

*"Em qualquer grupo de pessoas, todas as pessoas têm a mesma idade"*

**Demonstração:** *Por indução sobre o número de pessoas no grupo (em  $\mathbb{N}^*$ ).*

**Caso base** *num grupo de uma pessoa, todas as pessoas tem a mesma idade, trivialmente.*

**Caso do passo indutivo** *Hipótese de indução: todas as pessoas tem a mesma idade em qualquer grupo de  $n$  pessoas.*

*Seja  $G$  um grupo de  $n + 1$  pessoas, sejam  $G_1$  e  $G_2$  os grupos das  $n$  primeiras e últimas pessoas de  $G$ . Todas as pessoas de  $G_1$  e de  $G_2$  têm a mesma idade, por hipótese. Logo a primeira pessoa de  $G_1$  tem a mesma idade do que a segunda pessoa de  $G_1$ , essa segunda pessoa de  $G_1$  é a primeira pessoa de  $G_2$  e tem a mesma idade do que a última de  $G_2$ , logo a primeira pessoa de  $G$  ( $\in G_1, \notin G_2$ ) tem a mesma idade do que a última pessoa de  $G$  ( $\in G_2, \notin G_1$ ). Logo, todas as pessoas de  $G$  têm a mesma idade.*

**Conclusão** *Fica então demonstrado que em qualquer grupo de pessoas, todas as pessoas têm a mesma idade*

**Resposta**

□

**Exercício 36**

1. *Definir a função  $\text{subtermo}(t)$  que devolve o conjunto dos subtermos de um termo  $t \in T$ .*
2. *Definir a função  $\text{altura}(a)$  que devolve a altura de uma árvore  $a \in AB_A$ .*
3. *Definir a função  $\text{nós}(a)$  que devolve o número de nós da árvore parâmetro  $a \in AB_A$ .*

4. Definir a função  $folhas(a)$  que devolve o número de folhas da árvore parâmetro  $a \in AB_A$ .
5. Definir a função  $pot(x, n)$  que devolve  $x^n$  ( $n \in \mathbb{N}$ ).
6. Definir a função  $pertence(x, l)$  que devolve 1 se  $x \in A$  pertence a  $l \in L_A$ , 0 senão.
7. Definir a função  $comprimento(l)$  que devolve o tamanho da lista  $l \in L_A$ .
8. Definir a função  $inverte(l)$  que devolve a lista inversa a lista  $l \in L_A$  (a lista em que os elementos estão em ordem inversa em comparação a  $l$ ).
9. Definir a função  $concat(l_1, l_2)$  que concatena a lista  $l_2$  a lista  $l_1$  ( $l_1, l_2 \in L_A$ ).

□

**Exercício 37** Uma árvore binária é estrita se não tiver um nó com um só filho e se não for a árvore vazia.

1. Dar a definição indutiva de  $ABs_A$ , o conjunto das árvores binárias estritas.
2. Mostrar que em  $ABs_A$  se tem  $n(x) = 2 * f(x) - 1$  em que  $x$  é um elemento de  $ABs_A$ ,  $n$  a função que devolve o número de nós de uma árvore, e  $f$  a função que devolve o número de folhas de uma árvore.

□

**Exercício 38**

- a) Definir a linguagem  $T$  de termos baseada no alfabeto  $F = F_0 \cup F_2$  onde  $F_0 = \{c\}$  e  $F_2 = \{f\}$ .
- b) Dado a interpretação  $h$  em  $\mathbb{N}$  seguinte,

$$h(c) = 1 \tag{3}$$

$$h_f(n, m) = n + m \tag{4}$$

que conjunto  $X$  é definido por  $X = \{h^*(t) \mid t \in T\}$ ?

c) Será a definição de  $X$ , correspondente a  $T$ , ambígua?

□

**Exercício 39** Seja  $\mathbb{N}^* = \mathbb{N}/\{0\}$  Seja a definição seguinte de  $\text{modulo}(n, m)$  no conjunto indutivo  $\mathbb{N} \times \mathbb{N}^*$  por

$$\text{modulo}(n, m) = \begin{cases} n & \text{se } n < m \\ \text{modulo}((n - m), m) & \text{senão} \end{cases}$$

Esta definição define modulo como uma função apesar de  $\mathbb{N} \times \mathbb{N}^*$  ser definido ambigualmente. Extrair uma definição não ambígua de  $\mathbb{N} \times \mathbb{N}^*$  que corresponde a função modulo.

□

**Exercício 40** • Definir  $\text{maxelem}(a)$  e  $\text{minelem}(a)$ ,  $a \in AB_A$ , as funções que devolvem o maior e menor elemento ( $\in A$ ) da árvore  $a$ .

- Definir o conjunto das árvores  $ABo_A$  das árvores ordenadas.
- Provar que o percurso infixo de uma árvore ordenada  $a$  devolve sempre a lista crescente dos elementos de  $a$ .

□

## 5 Indução Bem Fundada

**Exercício 41** Considere a sequência (de Fibonacci) de inteiros seguintes:

- $F_1 = F_2 = 1$
- $F_n = F_{n-1} + F_{n-2}$

Demonstre por indução bem fundada que  $F_n = \frac{1}{\sqrt{5}}(\Phi^n - \bar{\Phi}^n)$ , onde  $\Phi = \frac{1+\sqrt{5}}{2}$  e  $\bar{\Phi} = \frac{1-\sqrt{5}}{2}$ .

□

**Exercício 42** Demonstre que:

- a relação de inclusão é uma relação bem fundada;
- a relação  $\leq$  sobre  $\mathbb{N}$  é uma relação bem fundada



- a relação  $\leq_{div}$  sobre  $\mathbb{N}^*$  é uma relação bem fundada

**Resposta**

- a relação  $\leq$  sobre  $\mathbb{Z}$  não é uma relação bem fundada

□

**Exercício 43** 1. Mostre que  $\forall n \in \mathbb{N}. (n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4) = 4$

2. Deduzir que qualquer inteiro  $m$  pode ser escrito como soma e diferença dos quadrados  $1^2, 2^2, 3^2, \dots, n^2$  para um determinado  $n$ . Isto é:

$$\forall m \in \mathbb{N}. \exists n \in \mathbb{N}. \exists \epsilon_1, \dots, \epsilon_n \in \{-1, 1\}. m = \epsilon_1 \cdot 1^2 + \epsilon_2 \cdot 2^2 + \dots + \epsilon_n \cdot n^2$$

□

**Exercício 44** Sejam  $(A, \leq_A)$  e  $(B, \leq_B)$  dois conjuntos **ordenados** por ordens largas **totais** e **bem fundadas** (diz-se, neste caso, que  $\leq_A$  e  $\leq_B$  são boas ordens). Seja  $(A \times B, \leq^{\mathcal{L}})$  o conjunto  $A \times B$  ordenado pela ordem lexicográfica  $\leq^{\mathcal{L}}$  i.e.

$$(a, b) \leq^{\mathcal{L}} (c, d) \triangleq \begin{cases} (a <_A c) \\ (a = c) \wedge (b \leq_B d) \end{cases}$$

onde  $(a <_A c) \triangleq (a \leq_A c) \wedge (a \neq c)$ . Demonstre que  $(A \times B, \leq^{\mathcal{L}})$  é bem fundado.

**Resposta** □

**Exercício 45** Seja  $d$  a função OCaml seguinte:

```

1 let rec d x y =
2   if x < y then 0
3   else if y = 0 then x
4         else (d (x-y) y) +1 ;;

```

1. Diga, **brevemente**, o que calcula a função  $d$ .
2. Demonstre, por indução bem fundada, que a função  $d$  termina.

Resposta

□

**Exercício 46** *Sejam misterio a seguinte função OCaml.*

```
1 let rec misterio f e l a =
2   match l with
3     [] → a
4   | el::li →
5       let (a1,a2)=a in
6         if (f el e)
7           then misterio f e li (el::a1,a2)
8           else misterio f e li (a1,el::a2)
```

1. Diga o que calcula a função misterio. Considere por exemplo a execução de  $\text{misterio } (<) 4 [3; 7; 4; 1; 8] ([], [])$ .
2. Demonstre a terminação da função misterio. Para tal, assumo que a função parâmetro  $f$  termina.

Resposta □

**Exercício 47** *Seja  $f$  a função OCaml seguinte:*

```
let rec f x =
  if (x<1)
  then 0
  else
    if (x=1)
    then 1
    else (f (x-2))*(f (x-1))/2
```

*Demonstre, usando a indução bem fundada, que  $\forall n \in \mathbb{N}$ .  $(f n)$  termina.*

□

**Exercício 48** *Diga, dos conjuntos ordenados seguintes, quais são os conjuntos ordenados bem fundados. No caso negativo apresenta uma justificação formal (um contra-exemplo por exemplo). Considere  $\leq$  como a relação de ordem habitual e  $|$  como a relação de divisibilidade (i.e.  $a|b \triangleq a$  divide  $b$ );*

1.  $(\mathbb{N}, \leq)$ ;

2.  $(\mathbb{Z}, \leq)$  ;
3.  $(\mathbb{N}, |)$  ;
4.  $(\mathbb{R}, \leq)$  ;
5.  $(\{2n \mid n \in \mathbb{N}^*\}, |)$
6.  $(\{2^n \mid n \in \mathbb{N}^*\}, |)$
7.  $\forall C$  conjunto,  $(\wp(C), \subseteq)$

□

**Exercício 49** *Sejam  $(A, \leq_A)$  e  $(B, \leq_B)$  dois conjuntos **ordenados** por ordens largas **totais** e **bem fundadas** (diz-se, neste caso, que  $\leq_A$  e  $\leq_B$  são boas ordens). Seja  $(A \times B, \leq^{\mathcal{L}})$  o conjunto  $A \times B$  ordenado pela ordem lexicográfica  $\leq^{\mathcal{L}}$  i.e.*

$$(a, b) \leq^{\mathcal{L}} (c, d) \triangleq \begin{cases} (a <_A c) \\ (a = c) \wedge (b \leq_B d) \end{cases}$$

onde  $(a <_A c) \triangleq (a \leq_A c) \wedge (a \neq c)$ . *Demonstre que  $(A \times B, \leq^{\mathcal{L}})$  é bem fundado.*

□

**Exercício 50** *Sejam  $(A, \leq_A)$  e  $(B, \leq_B)$  dois conjuntos **ordenados bem fundados**. Seja  $(A \times B, \leq_{A \times B})$  o conjunto  $A \times B$  ordenado pela ordem produto  $\leq_{A \times B}$  i.e.  $(a, b) \leq_{A \times B} (c, d) \triangleq ((a \leq_A c) \wedge (b \leq_B d))$ . *Demonstre que  $(A \times B, \leq_{A \times B})$  é igualmente bem fundado. Para tal considere a definição da noção de ordem bem fundada e verifique que  $\leq_{A \times B}$  respeita bem esta definição (uma demonstração possível é proceder por contradição).**

□

**Exercício 51** *Seja  $A^*$  o monóide livre gerado a partir do alfabeto  $A$ . Mostre que  $\forall u, v \in A^*, u.v = v.u \iff \exists w \in A^*. \exists p, q \in \mathbb{N}. u = w^p \wedge v = w^q$*

□

## 6 Técnica da Diagonal

**Exercício 52** *Demonstre, usando o princípio da diagonalização, que o conjunto  $\mathcal{F}$  das funções unárias de  $\mathbb{N}$  para  $\mathbb{N}$  não é numerável. Para tal, prossiga por contradição (assuma que  $\mathcal{F}$  é numerável) e considere a matriz  $M$  booleana cujas linhas são as funções  $f_0, f_1, \dots, f_i, \dots$  de  $\mathcal{F}$  e as colunas os inteiros de  $\mathbb{N}$ , ou seja,  $0, 1, 2, \dots, i, \dots$ . Que significado atribuir a  $M(f_i, k) = \text{true}$ ? Neste caso, que representa o conjunto diagonal? Conclua.*  $\square$

**Exercício 53** *Seja  $\mathbb{B}$  o conjunto de todas as seqüências infinitas de  $\{0, 1\}$ . Mostre que este conjunto não é numerável.*

*Sugestão: assumo que exista uma enumeração destas seqüências e crie uma matriz (para exibir a diagonal) em que se troca o  $i$ -ésimo bit da  $i$ -ésima seqüência.*

$\square$

**Exercício 54** *Demonstre que  $[0, 1]$  não é numerável.*

*Sugestão. É bem conhecido que tais reais se podem traduzir em seqüências infinitas binárias ...*

$\square$