Notas de

Matemática Discreta

LURDES SOUSA

Departamento de Matemática

Escola Superior de Tecnologia de Viseu

Instituto Politécnico de Viseu

Primeira edição: 2006
Última revisão (em construção): 2012

Índice

Capítulo I

Cálculo Proposicional

1 Proposições e conectivos lógicos

Consideremos os raciocínios seguintes:

a) – O livro é do João ou do Rui.

– O livro não é do Rui.

– Logo é do João.

b) – Se ela foi ao Egipto então esteve no Cairo.

– Ela não esteve no Cairo.

– Logo não foi ao Egipto.

c) – Ele pratica futebol e ténis.

– Logo ele pratica futebol.

Estes raciocínios são constituídos por afirmações que são verdadeiras ou falsas. Acerca de cada um deles é fácil concluir de que se trata de um raciocínio correcto. Grande parte das nossas operações mentais no dia a dia envolvem raciocínios deste tipo. Eles vão ser objecto de estudo no que se segue.

Chama-se *proposição* a uma expressão da qual faz sentido dizer que é verdadeira ou que é falsa.

Cada proposição tem um e um só *valor lógico*, entre dois possíveis, **V** (verdadeiro) ou **F** (falso).

1.1 Exemplos. "Lisboa é uma cidade portuguesa."é uma proposição com valor lógico verdadeiro. Mas atribuir um valor lógico à afirmação "Hoje está um belo dia!"já não faz sentido, pois trata-se da expressão de um sentimento de alguém, não de uma afirmação objectiva.

A lógica que vamos estudar pressupõe os seguintes princípios:

Princípio da não contradição: Uma proposição não pode ser verdadeira e falsa ao mesmo tempo.

Princípio do terceiro excluído: Uma proposição é verdadeira ou falsa.

A afirmação “O livro é do João ou do Rui.”pode decompor-se em duas afirmações: “O livro é do João.”e “O livro é do Rui.”Estas duas últimas afirmações já não se podem decompor. Dizemos então que a proposição ‘O livro é do João ou do Rui.”é composta e as afirmações “O livro é do João.”e “O livro é do Rui.”são atómicas.

A afirmação “Ela não esteve no Cairo.”é a negação de “Ela esteve no Cairo.”Construimos proposições compostas a partir de proposições atómicas ligando-as por conectivos. Se denotarmos por p a proposição “Ela esteve no Cairo.”e usarmos o símbolo $\neg$ para representarmos a negação, a afirmação “Ela não esteve no Cairo.”escreve-se $\neg p$. Temos assim a operação “negação”.

Analogamente, usando $\vee$ para representar “ou”, e as letras p e q para designar as proposições atómicas de “O livro é do João ou do Rui.”, obtemos, simbolicamente, $p \vee q$. Trata-se aqui da operação “disjunção”.

A seguir apresenta-se uma lista destas e doutras operações lógicas:

negação:	$\neg p$	(não p)
conjunção:	$p \wedge q$	(p e q)
disjunção:	$p \vee q$	(p ou q)
implicação:	$p \rightarrow q$	(se p então q; p só se q; p é condição suficiente para que q; q é condição necessária para que p)
equivalência (formal): (bicondicional)	$p \leftrightarrow q$	(p equivalente a q)
disjunção exclusiva:	$p \dot{\vee} q$	(ou p ou q)

Quando temos uma implicação $p \rightarrow q$ dizemos que p é o *antecedente* e q o *consequente*.

As operações anteriores têm tabelas de valores que vão ao encontro do significado habitual das partículas "não", "e", "ou", etc. Essas tabelas apresentam-se de seguida. (Certifique-se de que compreende a forma natural como surgem estas tabelas, de acordo com o nosso entendimento da linguagem do dia-a-dia.)

Tabelas de verdade das operações lógicas

Uma tabela de verdade faz corresponder aos possíveis valores lógicos das variáveis o correspondente valor lógico da expressão. Seguem-se as tabelas das operações lógicas enumeradas atrás.

p	$\neg p$
V	F
F	V

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

p	q	$p \dot{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

Lógica e operações-*bit*:

Os computadores representam informação por meio de *bits*. Um *bit* tem dois valores possíveis, 0 e 1. Um *bit* pode ser usado para representar os valores de verdade **F** e **V**, 0 representa **F** e 1 representa **V**. Uma variável diz-se booleana se o seus valores possíveis são **V** ou **F** (ou, se quisermos, 1 ou 0). Portanto, uma variável booleana pode ser representada por meio de um *bit*.

1.2 Exercícios.

1. Quais das seguintes frases são proposições?

   (a) Isto é verdade? (b) João é um nome.
   (c) 8 é um número ímpar. (d) 8 é um número par. (e) Esta cor é bonita.

2. Indique os valores lógicos das proposições seguintes:

   (a) 7 é um número primo. (b) Lisboa é uma cidade. (c) Canadá é uma cidade.

3. Diga quais das seguintes proposições são atómicas e quais são compostas:

   (a) O Frederico é alto, e o Joaquim também. (b) O carro acidentado era azul ou verde.
   (c) O carro acidentado era meu. (d) Se fores ao bar, então eu vou ao bar.

4. Usando os símbolos e e a para "Manuel é estudante" e "Manuel joga andebol", respectivamente, escreva as seguintes afirmações na forma simbólica:

   (a) Manuel é estudante. (b) Manuel é estudante e joga andebol.
   (c) Manuel é estudante ou joga andebol. (d) Se Manuel é estudante, então joga andebol.

5. Identifique todas as proposições atómicas nas frases seguintes e represente-as por símbolos p, q, r, etc. Em seguida escreva as frases sob a forma de cálculo proposicional.

   (a) Se a Maria está no ginásio, então a Marta também está no ginásio.
   (b) O carro do Rui é vermelho ou castanho.
   (c) Se te levantares às sete horas, chegarás a tempo.
   (d) Chegarás a tempo se e só se te levantares às sete horas.
   (e) Ele virá se tu o avisares.
   (f) É suficiente que o João tenha 9,5 para que passe.
   (g) Amanhã vou de autocarro ou de táxi.
   (h) Amanhã vou de autocarro se ele parar no Rossio, ou vou de táxi se tiver dinheiro.
   (i) Se acabar o meu trabalho vou para a praia se fizer bom tempo.

6. Escreva as tabelas de verdade para:

   (a) $p \vee (q \wedge r)$ (b) $\neg(\neg p \vee \neg q)$
   (c) $(\neg p \wedge (\neg q \wedge r)) \vee (q \wedge r) \vee (p \wedge r)$ (d) $(p \vee \neg q) \rightarrow (r \vee p)$
   (e) $(p \vee (q \wedge r)) \vee \neg((p \vee q) \wedge (r \vee s))$ (f) $(p \vee \neg q) \leftrightarrow (r \wedge p)$
   (g) $(p \leftrightarrow \neg q) \wedge (q \rightarrow p)$ (h) $((p \rightarrow q) \rightarrow q) \vee \neg p$

7. Escreva cada uma das seguintes proposições na forma simbólica.

   (a) Uma condição necessária para x ser primo é que x seja ímpar ou $x = 2$.
   (b) Uma condição suficiente para que f seja contínua é que f seja diferenciável.
   (c) Ele vai morrer hoje, a menos que consiga auxílio médico.
   (d) Se os impostos forem aumentados ou diminuirem os gastos governamentais, não haverá inflação.

8. Qual o valor de verdade das seguintes proposições?

   (a) O número 2 é primo ou 4 é ímpar.
   (b) O número 2 não é primo e 4 é ímpar.
   (c) O número 2 é primo e 4 é ímpar.
   (d) O número 2 não é primo ou 4 é ímpar.
   (e) Se 2 não for primo então 4 é ímpar.
   (f) Se 2 for primo então 4 é ímpar.
   (g) Se 2 não for primo então 4 é par.
   (h) Se 2 não for primo e 4 for par então $4 < 2$.

9. Escreva a negação das proposições (a), (b), (c) e (i) do exercício 5.

10. Escreva a recíproca das proposições (a), (e) e (i) do exercício 5.

11. Escreva cada uma das frases seguintes na forma de implicação ($p \to q$):

    (a) Se estragares o meu livro não volto a emprestar-to.
    (b) Toca nesse bolo e arrepender-te-ás.
    (c) Sai ou chamo a polícia.
    (d) Vou-me embora se não pararem de falar.

2 Fórmulas bem formadas e semântica

Relativamente a uma dada linguagem lógica podemos sempre estudar dois aspectos: a sintaxe e a semântica. A sintaxe diz respeito às regras de formação das expressões lógicas a utilizar, as chamadas fórmulas bem-formadas. A semântica estuda o significado dessas expressões.

Linguagem (conjunto de símbolos) ⟨ sintaxe (fórmulas bem-formadas) / semântica (significado)

Na linguagem do cálculo proposicional vamos considerar a sintaxe e a semântica seguintes.

<u>Sintaxe</u>:

Uma variável proposicional é um símbolo p, q, r, ... ao qual podemos atribuir o valor lógico V ou F. Uma *proposição atómica* ou *átomo* é uma variável proposicional ou uma constante, V ou F.

Uma *fórmula bem formada* (abreviadamente, *fbf*) fica definida da seguinte forma (supondo que consideramos apenas os conectivos lógicos $\neg$, $\wedge$, $\vee$ e $\to$):

- V e F são fbf's; toda a variável proposicional é uma fbf;
- Se A e B são fbf's, as seguintes são também fbf's:

$$\neg A$$

$$(A \wedge B)$$

$$(A \vee B)$$

$$(A \rightarrow B)$$

$$(A \leftrightarrow B)$$

- Toda a fbf é formada por estas regras.

Os parêntesis funcionam como símbolos auxiliares que indicam como é formada a fbf. Para evitar um uso excessivo de parêntesis e simplificar a escrita das expressões lógicas convenciona-se que as operações lógicas são consideradas pela seguinte ordem de prioridade:

$$\neg$$

$$\wedge$$

$$\vee$$

$$\rightarrow$$

$$\leftrightarrow$$

Atentando na definição de fbf acabada de dar, é fácil de ver que as expressões

$$p \vee \neg q \wedge r\,,\ (p \vee \neg q) \wedge r\,,\ \neg(p \rightarrow q \wedge r) \ \text{ e } \ \neg p \rightarrow q \wedge r$$

são fbf's, ao passo que as expressões

$$\neg \wedge p \vee q \ \text{ e } \ p \vee (\wedge q \rightarrow r)$$

o não são.

Se F é uma fbf da forma $\neg A$, A diz-se uma *subfórmula bem formada* (abreviadamente, *subfbf*) de F; analogamente se F é uma fbf da forma $A \wedge B$, $A \vee B$ ou $A \rightarrow B$, A e B dizem-se *subfbf*'s de F. Se C é uma subfbf de G e G é uma subfbf de F então C é uma subfbf de F.

Uma fbf que não seja proposição atómica diz-se *proposição composta*.

<u>Semântica</u>:

Dada uma fbf, atribuindo a cada uma das suas variáveis proposicionais o valor lógico V ou F, obtemos uma interpretação (significado) para a fbf. As interpretações possíveis podem dispôr-se numa tabela, chamada *tabela de verdade* da fbf. O Exemplo 2.1 contém a tabela de verdade de $p \to p \vee q$.

Uma fbf diz-se uma *tautologia* se for verdadeira para todos os possíveis valores lógicos dos átomos.

Uma fbf diz-se uma *contradição* se for falsa para todos os possíveis valores lógicos dos átomos.

Uma fbf diz-se uma *contingência* se não for nem tautologia nem contradição.

2.1 Exemplo. Suponhamos que queremos averiguar se $p \to p \vee q$ é ou não uma tautologia. Para isso podemos utilizar uma tabela de verdade:

p	q	$p \vee q$	$p \to p \vee q$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

Como para quaisquer valores de p e q a fbf $p \to p \vee q$ toma sempre o valor de verdade, conclui-se que é uma tautologia.

Podemos também obter a resposta sem fazer uma tabela de verdade, basta raciocinar do seguinte modo: A implicação só é falsa quando o antecedente é verdadeiro e o consequente falso. Mas se p tomar o valor V também $p \vee q$ toma o valo V, obtendo-se $V \to V$ que é V. Logo $p \to p \vee q$ toma sempre o valor de verdade, pelo que é uma tautologia.

2.2 Exercícios.

1. Para cada uma das expressões seguintes diga se são ou não fórmulas bem-formadas.
   (a) $(p \neg q) \wedge p$ (b) $(\neg p \vee q) \wedge p$ (c) $p \vee \wedge q$

2. Ponha parênteses nas expressões seguintes de tal modo que sejam indicadas as regras de prioridade estabelecidas para os conectivos envolvidos.

   (a) $p \wedge q \wedge r \to p$ (b) $p \wedge r \vee q \leftrightarrow \neg r$
   (c) $\neg(p_1 \wedge p_2) \to \neg q \vee p_1$ (d) $p \to q \leftrightarrow \neg q \to \neg q$

3. Obtenha a fórmula bem-formada $p \vee \neg q \wedge (p \to r)$ usando as regras de formação de uma fórmula bem-formada descritas atrás.

4. Averiguar se a fbf $p \wedge q \wedge r \wedge s \wedge t \to \neg r$ é ou não uma tautologia.

5. Mostre que são tautologias:

   (a) $(p \leftrightarrow (p \wedge \neg p)) \leftrightarrow \neg p$ (b) $(p \to q) \to ((q \to r) \to (p \to r))$

6. Prove que $((p \wedge r) \vee (q \wedge \neg r)) \leftrightarrow ((\neg p \wedge r) \vee (\neg q \wedge \neg r))$ é uma contradição.

7. Diga quais das seguintes fórmulas são tautologias, contradições, ou nem uma coisa nem outra.

   (a) $((p \to q) \to \neg(q \to p)) \leftrightarrow (p \leftrightarrow q)$ (b) $((p \to q) \to q) \to q$

   (c) $((p \to q) \to p) \leftrightarrow (q \to (q \to p))$ (d) $(p \to (q \wedge \neg q)) \to \neg p$

3 Equivalência Lógica

Duas fbf's dizem-se *(logicamente) equivalentes* se tiverem o mesmo significado, isto é, a mesma tabela de verdade. Para indicar que duas fbf's A e B são equivalentes, escrevemos

$$A \equiv B\,.$$

Em vez do símbolo $\equiv$ também se usa $\Leftrightarrow$. Note-se que dizer que A e B são logicamente equivalentes é o mesmo que dizer que $A \leftrightarrow B$ é uma tautologia.

Algumas equivalências básicas:

$p \vee \neg p \equiv V$	Lei do terceiro excluido
$p \wedge \neg p \equiv F$	Lei da contradição
$p \wedge V \equiv p$ $p \vee F \equiv p$	Leis da identidade
$p \vee V \equiv V$ $p \wedge F \equiv F$	Leis da absorção
$p \vee p \equiv p$ $p \wedge p \equiv p$	Leis da idempotência
$\neg(\neg p) \equiv p$	Lei da dupla negação
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Leis da comutatividade
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Leis da associatividade
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Leis da distributividade
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	Leis de De Morgan

Todas estas equivalências são de fácil verificação. Por exemplo, construindo as tabelas de verdade de $\neg(p \wedge q)$ e $\neg p \vee \neg q$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
V	V	V	F	F	F	F
V	F	F	V	F	V	V
F	V	F	V	V	F	V
F	F	F	V	V	V	V

concluimos que ambas as fbf's têm o mesmo valor lógico para os mesmos valores das variáveis proposicionais, logo são logicamente equivalentes.

Tendo em conta a definição de equivalência lógica entre fbf's, é fácil concluir que:

> *Se numa fbf substituirmos uma subfbf por uma fbf equivalente obtemos uma fbf equivalente à fbf original.*

Esta regra aplica-se quando pretendemos simplificar fbf's. Por exemplo, como sabemos que $p \vee p \equiv p$, concluimos que $(p \vee p) \wedge q \equiv p \wedge q$.

É muitas vezes útil utilizar as seguintes equivalências (verifique-as):
$p \rightarrow q \equiv \neg p \vee q$
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Associadas a uma implicação $p \rightarrow q$ temos as duas fbf's seguintes:
(a) $q \rightarrow p$, que se diz a *recíproca* de $p \rightarrow q$;
(b) $\neg q \rightarrow \neg p$, que se diz a *contrapositiva* de $p \rightarrow q$.

3.1 Exercícios.

1. Mostre que $p \rightarrow q$ é logicamente equivalente à sua contrapositiva mas não é logicamente equivalente à sua recíproca.

2. Use propriedades das conjunção, disjunção e negação para provar as seguintes equivalências:

   (a) $(p \wedge q) \vee (q \wedge r) \equiv q \wedge (p \vee r)$

   (b) $\neg(\neg(p \wedge q) \vee p) \equiv \mathrm{F}$

   (c) $\neg(\neg p \vee \neg(r \vee s)) \equiv (p \wedge r) \vee (p \wedge s)$

   (d) $(p \vee r) \wedge (q \vee s) \equiv (p \wedge q) \vee (p \wedge s) \vee (r \wedge q) \vee (r \wedge s)$

3. Simplifique as expressões seguintes:

   (a) $(p \wedge \mathrm{V}) \wedge (q \wedge \mathrm{V})$

   (b) $(r \wedge (q \wedge (p \wedge r)))$

   (c) $(r \wedge \mathrm{V}) \wedge (q \wedge \neg r)$

   (d) $(q \wedge r \wedge s) \vee (q \wedge \neg r \wedge s)$

   (e) $(p \vee r) \wedge (p \vee r \vee s)$

   (f) $(p \vee (q \wedge s)) \vee (\neg q \wedge s)$

   (g) $p \vee \neg q \vee (p \wedge q) \wedge (p \vee \neg q) \wedge \neg p \wedge q$

   (h) $\neg((p \vee q) \wedge r) \vee q$

   (i) $(p \vee \neg q) \wedge (\neg p \vee q) \vee \neg(\neg(p \vee \neg r) \wedge q)$

4. Construa para cada caso proposições compostas P e Q por forma a que as proposições apresentadas sejam tautologias:

   (a) $P \ \wedge Q$ (b) $P \rightarrow \neg P$

5. Use a tautologia $p \vee \neg p$ para provar que as seguintes proposições são tautologias.

   (a) $(p \rightarrow q) \vee \neg(p \rightarrow q)$ (b) $\neg p \vee \neg\neg p$ (c) $((p \wedge s) \vee q) \vee \neg((p \wedge s) \vee q)$

6. Mostre que a fórmula $(\neg p \rightarrow q) \rightarrow (p \rightarrow \neg q)$ não é uma tautologia. Encontre fórmulas ϕ e ψ tais que $(\neg\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \neg\psi)$ seja uma contradição.

7. Mostre que $(p \rightarrow q) \wedge (\neg p \rightarrow q) \rightarrow q$ é uma tautologia e use esta tautologia para provar que $(\neg p \rightarrow \neg q) \wedge (\neg\neg p \rightarrow \neg q) \Rightarrow \neg q$.

8. Determine expressões logicamente equivalentes às seguintes mas sem os conectivos $\rightarrow$ e $\leftrightarrow$:

   (a) $(p \rightarrow q) \vee (q \rightarrow r)$ (b) $(p \rightarrow q) \leftrightarrow (p \wedge q \leftrightarrow q)$ (c) $\neg p \rightarrow \neg q$

4 Argumentos correctos

No nosso dia a dia raciocinamos e tiramos conclusões usando determinadas regras. A lógica ajuda a compreender essas regras permitindo distinguir entre argumentos correctos e não correctos. Seguem-se alguns argumentos lógicos, cada um deles com um exemplo e a respectiva formalização.

1)

1. Se o gato vê o peixe, então o gato apanha o peixe.
2. Se o gato apanha o peixe, então o gato come o peixe.

---

3. Se o gato vê o peixe, então o gato come o peixe.

1. $p \to q$
2. $q \to r$

---

3. $p \to r$

2)

1. Se o João tem mais de 16 anos, então vai ao cinema.
2. O João tem mais de 16 anos.

---

3. O João vai ao cinema.

1. $p \to q$
2. p

---

3. q

3)

1. A Maria traz as bebidas ou faz um bolo.
2. A Maria não faz um bolo.

---

3. A Maria traz as bebidas.

1. $p \vee q$
2. $\neg q$

---

3. p

Um argumento da forma "De A_1, A_2, ... e A_n deduz-se B.", esquematicamente,

$$\begin{array}{c} A_1 \\ A_2 \\ . \\ . \\ . \\ A_n \\ \hline B \end{array}$$

diz-se um *argumento correcto* se $A_1 \wedge A_2 \wedge ... \wedge A_n \to B$ for uma tautologia. Neste caso escrevemos

$$A_1, A_2, ..., A_n \models B$$

Para indicar que $P \models Q$ também se usa $P \Rightarrow Q$, nomenclatura que faz parte do dia a dia da escrita matemática.

4.1 Exercícios.

1. Use os símbolos proposicionais p e q para formalizar os seguintes argumentos lógicos:

   (a) Se 10 é um número primo, 10 não pode ser igual a 2 vezes 5. 10 é igual a 2 vezes 5. Logo, 10 não pode ser um número primo.

   (b) Se chove frequentemente, os agricultores queixam-se. Se não chove frequentemente, os agricultores queixam-se. Consequentemente, os agricultores queixam-se.

   (c) O António almoça na cantina ou o António almoça em casa. O António não almoça na cantina. Logo, o António almoça em casa.

2. Verifique se o argumento seguinte está correcto (i. e., se a conclusão é logicamente implicada pela conjunção das hipóteses).

   "Se o orçamento não for cortado, uma condição necessária e suficiente para os preços permanecerem estáveis é que os impostos sejam aumentados. Os impostos serão aumentados somente se o orçamento não for cortado. Se os preços permanecerem estáveis, os impostos não serão aumentados. Portanto os impostos não serão aumentados."

3. Mostre que os seguintes argumentos são correctos, usando tabelas de verdade.

   (a) $p \vee q, \neg p \vee r \models q \vee r$ (b) $p \to q, p \to r \models p \to q \wedge r$

   (c) $p, p \to q \models p \wedge q$ (d) $p \vee q, p \to r, q \to r \models r$

4. Num certo país cada habitante diz sempre a verdade ou diz sempre a mentira. Um viajante nesse país encontra o Pedro e a Luísa. O Pedro disse-lhe: "Se eu digo sempre a verdade, então a Luísa também diz sempre a verdade." Será Pedro um mentiroso ou, pelo contrário, diz sempre a verdade? E a Luísa?

   Nesse mesmo país, o viajante encontrou o António e o Manuel e este último disse-lhe: "Se eu sou mentiroso então o António também é mentiroso."Que pode concluir quanto a cada um deles ser ou não dos que dizem sempre a verdade?

5 Formas normais

Uma *função de verdade* (ou *função lógica*) é uma função que só pode tomar os valores lógicos V ou F e cujos argumentos também só podem tomar esses valores. Por exemplo,

$$f(p,q) = \begin{cases} \text{V se } p \text{ é V} \\ \text{V se } p \text{ e } q \text{ são ambas F} \\ \text{F se } p \text{ é F e } q \text{ é V} \end{cases}$$

define uma função de verdade.

A seguir vamos ver que

Toda a função de verdade é equivalente a uma fbf.

Para isso vamos usar as definições que se seguem.

Um *literal* é uma variável proposicional ou a sua negação. Exemplos: p e $\neg p$. As duas expressões, p e $\neg p$ dizem-se *literais complementares.*

Uma fbf diz-se uma *forma normal disjuntiva (FND)* se for uma disjunção de conjunções de literais, ou se for V ou F.

Analogamente, uma fbf diz-se uma *forma normal conjuntiva (FNC)* se for uma conjunção de disjunções de literais, ou se for V ou F.

Exemplos de formas normais disjuntivas:

$$p$$

$$\neg p$$

$$p \vee \neg q$$

$$\neg p \wedge q$$

$$(p \wedge q) \vee (p \wedge \neg q)$$

$$p \vee (p \wedge r)$$

Exemplos de formas normais conjuntivas:

$$p$$

$$\neg p$$

$$p \wedge \neg q$$

$$\neg p \vee q$$

$$p \wedge (q \vee r)$$

Tabelas de verdade e formas normais:

Suponhamos que temos uma função de verdade f dada pela tabela de verdade

p	q	r	f
V	V	V	V
V	V	F	F
V	F	V	V
V	F	F	F
F	V	V	F
F	V	F	F
F	F	V	V
F	F	F	F

e que pretendemos escrever f como a disjunção de conjunções de literais, portanto, como uma forma normal disjuntiva. Ora, pela tabela de verdade de f, sabemos que f é verdadeira para cada um dos casos seguintes:

- p, q e r verdadeiras
- p, $\neg q$ e r verdadeiras
- $\neg p$, $\neg q$ e r verdadeiras

Então, tendo em conta que a disjunção de um número finito de fbf's é **V** se e só se uma delas o for, concluimos que

$$f \equiv (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge r)\,.$$

Ou seja, f é **V** se e só se

$$p \wedge q \wedge r \equiv \mathbf{V} \;\text{ ou }\; p \wedge \neg q \wedge r \equiv \mathbf{V} \;\text{ ou }\; \neg p \wedge \neg q \wedge r \equiv \mathbf{V}.$$

Por outro lado, f é falsa para

- $\neg p$, $\neg q$ e r falsas
- $\neg p$, q e r falsas
- p, $\neg q$ e $\neg r$ falsas
- p, $\neg q$ e r falsas
- p, q e r falsas

Então, atendendo a que a conjunção de fbf's é falsa se e só se uma delas é falsa, concluimos que

$$f \equiv (\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee r)\,.$$

O que acabámos de fazer para este exemplo pode ser feito para qualquer função de verdade; antes da descrição do procedimento geral a seguir, vamos definir termos mínimos e máximos.

Seja f uma fbf. Um *termo mínimo* (*termo máximo*, respectivamente) de f é uma conjunção (respectivamente, disjunção) de literais onde as variáveis são as de f e cada uma delas é representada uma e uma só vez.

Por exemplo, se as variáveis de f são p, q e r, alguns dos termos mínimos de f são

$$p \wedge \neg q \wedge r$$

$$\neg p \wedge q \wedge r$$

$$p \wedge q \wedge r$$

mas fbf's como $p \wedge q$ e $p \wedge \neg r$ não são termos mínimos de f.

De um modo geral, dada a tabela de verdade de uma fbf f, procedemos do seguinte modo para obter uma forma normal disjuntiva (respectivamente, conjuntiva) de f:

> Seleccionamos os termos mínimos (respectivamente, termos máximos) de f que tornam f verdadeira (respectivamente, falsa) e formamos a disjunção (respectivamente, conjunção) destes termos mínimos.

Uma fórmula proposicional f diz-se escrita na *forma normal disjuntiva plena* (respectivamente, *forma normal conjuntiva plena*) se estiver expressa como uma disjunção (respectivamente, conjunção) de termos mínimos (respectivamente, máximos) de f.

Portanto, no exemplo anterior, obtivemos uma forma normal disjuntiva plena e uma forma normal conjuntiva plena.

<u>Obtenção de formas normais através de manipulações algébricas</u>:

Suponhamos que queremos obter uma forma normal conjuntiva para a fbf $p \to (q \wedge r)$. Podemos fazer a respectiva tabela de verdade e proceder como descrito acima. Mas também podemos usar as equivalências lógicas já conhecidas:

$$p \to (q \wedge r) \equiv \neg p \vee (q \wedge r) \equiv (\neg p \vee q) \wedge (\neg p \vee r)$$

Chegámos assim a uma forma normal conjuntiva (não plena) da fbf dada por maio de manipulações algébricas. A seguir descreve-se o procedimento geral para obter formas normais usando este processo.

- Para obter uma <u>forma normal conjuntiva</u>:

  1. "Tiram-se"todos os $\to$ e $\leftrightarrow$.

2. Se a expressão contém negações de conjunções ou negações de disjunções, fazem-se desaparecer usando as leis de De Morgan.
3. Agora basta usar as duas propriedades distributivas seguintes

$$a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$$

$$(a \wedge b) \vee c \equiv (a \vee c) \wedge (b \vee c)$$

- Para obter uma forma normal disjuntiva: Procede-se de forma análoga, usando agora no passo 3 as propriedades seguintes:

$$a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c)$$

$$(a \vee b) \wedge c \equiv (a \wedge c) \vee (b \wedge c)$$

Se f é uma fórmula proposicional onde só aparecem os conectivos lógicos $\neg$, $\wedge$ e $\vee$, a *dual de* f é a fórmula que se obtém de f substituindo cada V por F, cada F por V, cada $\wedge$ por $\vee$ e cada $\vee$ por $\wedge$.

Se f é uma fórmula proposicional, o *complemento de* f obtém-se formando primeiro o dual de f e depois substituindo todos os literais pelos seus complementos. De facto, o complemento de f é a negação de f.

Exemplo: Pretende-se negar $f = (p \wedge q) \vee \neg r$, usando complementação. Ora, a dual de f é $(p \vee q) \wedge \neg r$. Logo

$$\neg f \equiv (\neg p \vee \neg q) \wedge r\,.$$

5.1 Exercícios.

1. Encontre uma fórmula restrita (i.e., contendo apenas os conectivos $\neg$, $\wedge$ e $\vee$) correspondente à função de verdade $f(p, q, r)$ dada na seguinte tabela:

p	q	r	$f(p,q,r)$
V	V	V	V
F	V	V	F
V	F	V	F
F	F	V	F
V	V	F	F
F	V	F	F
V	F	F	V
F	F	F	F

2. Determine a forma normal conjuntiva das seguintes expressões:

   (a) $(p \to q) \leftrightarrow (p \to r \vee q)$ (b) $(p \vee q) \wedge (p \vee (r \wedge s)) \vee (p \wedge q \wedge s)$

3. Determine uma forma normal disjuntiva e uma forma normal conjuntiva logicamente equivalente à fórmula $(p \to q) \to r$.

4. Seja f a função lógica dada pela tabela seguinte:

p	q	r	$f(p,q,r)$
F	F	F	F
F	F	V	V
F	V	F	F
F	V	V	F
V	F	F	V
V	F	V	F
V	V	F	F
V	V	V	V

   (a) Determine a forma normal disjuntiva de f.

   (b) Determine a forma normal conjuntiva de f.

6 Conjuntos de conectivos lógicos completos

Os conectivos lógicos habitualmente usados para formar as fbf's do cálculo proposicional são $\neg$, $\wedge$, $\vee$ e $\to$. É sabido que qualquer fbf pode ser substituída por outra logicamente equivalente e onde não figura o símbolo $\to$.

Um conjunto de conectivos lógicos diz-se *completo* se toda a fbf do cálculo proposicional é logicamente equivalente a uma fbf onde figuram apenas conectivos desse conjunto. Assim, $\{\neg, \wedge, \vee\}$ é completo.

6.1 Exercícios.

1. Mostre que cada um dos seguintes conjuntos de conectivos é completo para o cálculo proposicional:

   (a) $\{\neg, \to\}$ (b) $\{\neg, \wedge\}$ (c) $\{\neg, \vee\}$

2. Determine fórmulas logicamente equivalentes a $p \to q$

   (a) usando apenas o conectivo $|$ ($p|q$ é logicamente equivalente a $\neg(p \wedge q)$);

(b) usando apenas o conectivo $\downarrow$ ($p \downarrow q$ é logicamente equivalente a $\neg(p \vee q)$).

3. Suponha que o argumento $\phi_1, \phi_2, \ldots, \phi_n \models \phi$ é válido. Prove que $\phi_1, \phi_2, \ldots, \phi_{n-1} \models \phi_n \to \phi$ é também um argumento válido.

4. O conectivo lógico conhecido por "ou exclusivo" e representado por $\dot{\vee}$, é definido pela seguinte tabela de verdade:

p	q	$p \dot{\vee} q$
V	V	F
V	F	V
F	V	V
F	F	F

   (a) Mostre que $p \dot{\vee} q$ é equivalente a $\neg(p \leftrightarrow q)$.

   (b) Construa a tabela de verdade para $(p \dot{\vee} q) \dot{\vee} r$.

5. Determine fórmulas contendo apenas os conectivos $\neg$ e $\to$ logicamente equivalentes a

   (a) $(p \wedge q) \vee (r \wedge s)$ (b) $p \leftrightarrow q$

6. Mostre que qualquer fbf do cálculo proposicional é logicamente equivalente a uma fbf contendo apenas o conectivo lógico $\to$. (Sugestão: Use a constante **F** para expressar $\neg p$ por meio da implicação.)

7 Sistemas formais

Um *sistema formal S* consiste em:

1. Um conjunto (numerável) de *símbolos*.

2. Um conjunto de sequências finitas destes símbolos que constituem as chamadas *fórmulas bem formadas* (abreviadamente fbf).

3. Um subconjunto de fbf's chamadas *axiomas*.

4. Um conjunto finito de "regras de dedução"chamadas *regras de inferência* que permitem deduzir uma fbf como consequência directa de um conjunto finito de fbf's.

Seja S um sistema formal. Seja C um conjunto de fbf's e seja P uma fbf em S.

P é deduzível de C em S, e escreve-se

$$C \vdash_S P$$

(ou apenas $C \vdash_S P$ se não houver dúvidas sobre o sistema $\mathcal{S}$ a que nos referimos) se existir uma sequência finita de fbf's, $P_1, P_2, ..., P_n$ tais que:

- $P_n = P$
- Para cada $i \in \{1, ...n\}$, P_i é um axioma ou uma fbf em C (dita *premissa* ou *hipótese*) ou uma consequência dos P_i's anteriores através de uma das regras de inferência.

A sequência dos P_i's diz-se uma *prova formal* (ou *demonstração formal*) de P a partir de C.

Se P é deduzível de um conjunto vazio escreve-se

$$\vdash_S P$$

Neste caso, P diz-se um *teorema* em S.

Associada a um sistema formal podemos ter uma semântica (interpretação) que permite que cada fbf possa ser considerada como verdadeira ou falsa de acordo com a interpretação das suas variáveis.

Um sistema formal S diz-se:

Completo, se toda a fbf que é verdadeira para todas as interpretações possíveis pode ser demonstrada em S;

Coerente (ou sólido ou correcto), se toda a fbf que pode ser demonstrada em S é verdadeira para todas as interpretações.

Vamos a seguir descrever um sistema formal natural e um sistema formal de Hilbert, o que certamente ajudará a compreender a noção de sistema formal acabada de dar.

Sistema formal natural $\mathcal{L}$

1. Símbolos:

   a) variáveis proposicionais

   b) conectivos lógicos: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

   c) símbolos auxiliares: (e)

2. Fórmulas bem formadas: de acordo com o definido atrás.

3. Axiomas: não tem.

4. Regras de inferência: as da Tabela RI.

Tabela RI

$A, B \vdash A \wedge B$	Lei da combinação
$A \wedge B \vdash B$	Lei da simplificação
$A \wedge B \vdash A$	Variante da lei da simplificação
$A \vdash A \vee B$	Lei da adição
$B \vdash A \vee B$	Variante da lei da adição
$A, A \rightarrow B \vdash B$	Modus ponens
$\neg B, A \rightarrow B \vdash \neg A$	Modus tollens
$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$	Silogismo hipotético
$A \vee B, \neg A \vdash B$	Silogismo disjuntivo
$A \vee B, \neg B \vdash A$	Variante do silogismo disjuntivo
$A \rightarrow B, \neg A \rightarrow B \vdash B$	Lei dos casos
$A \leftrightarrow B \vdash A \rightarrow B$	Eliminação da equivalência
$A \leftrightarrow B \vdash B \rightarrow A$	Variante da eliminação da equivalência
$A \rightarrow B, B \rightarrow A \vdash A \leftrightarrow B$	Introdução da equivalência
$A, \neg A \vdash B$	Lei da inconsistência

Um teorema muito útil é o seguinte:

Teorema da Dedução. Sejam A, B, A_1, A_2, ..., A_n fórmulas bem formadas.
Se

$$A_1\, A_2,\, ...,\, A_n, A \vdash B$$

então

$$A_1,\, A_2,\, ...,\, A_n \vdash A \to B\,.$$

Por outras palavras:
Se das premissas $A_1\, A_2$, ..., A_n e A deduzimos B então das premissas A_1, A_2, ..., A_n deduzimos $A \to B$.

As regras de inferência da Tabela RI juntamente com o Teorema da Dedução fazem de $\mathcal{L}$ um sistema completo, i. e., se $A \models B$, então $A \vdash B$. 0 sistema $\mathcal{L}$ é também correcto, i. e., se $A \vdash B$, então $A \models B$.

Consequentemente, A_1, A_2, ..., $A_n \vdash B$ se e só se $A_1 \wedge A_2 \wedge ... \wedge A_n \to B$ é uma tautologia; de igual modo uma fbf P é um teorema em $\mathcal{L}$ se e só se for uma tautologia.

7.1 Exemplos de demonstrações formais em $\mathcal{L}$:

Cada uma das propriedades da Tabela RI pode ser designada por uma abreviatura, por exemplo, MP para modus ponens, MT para modus tollens, e assim por diante. É esta abreviatura que se usa na justificação de cada um dos passos das demonstrações formais dos dois teoremas que se seguem.

Teorema: $A \vee B \vdash \neg A \to B$

Pelo Teorema da Dedução (TD) basta provar o seguinte

Teorema: $A \vee B$, $\neg A \vdash B$

Prova:

1. $A \vee B$	premissa
2. $\neg A$	premissa
3. B	l., 2. e SD

Teorema: $A \to (B \to C)$, $A \to B$, $A \vdash C$.

Prova:

1. $A \to (B \to C)$	premissa
2. $A \to B$	premissa
3. A	premissa
4. B	MP, 2. e 3.
5. $B \to C$	MP, 1. e 3.
6. C	MP, 4. e 5.

Aplicando o TD sucessivamente ao teorema anterior, obtém-se o

Teorema: $A \to (B \to C) \vdash (A \to B) \to (A \to C)$

Sistema formal de Hilbert $\mathcal{H}$

1. Símbolos
   (a) variáveis proposicionais
   (b) conectivos lógicos: $\neg$ e $\to$
   (c) símbolos auxiliares: (e)
2. Fórmulas bem formadas
   (a) fórmulas atómicas
   (b) fórmulas compostas: Se A e B são fbf então $\neg A$ e $A \to B$ são também fbf's.
3. Axiomas

   H1) $A \to (B \to A)$

   H2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

   H3) $(\neg A \to \neg B) \to ((\neg A \to B) \to A)$
4. Regras de inferência (só uma):

   Modus Ponens (MP): $A, A \to B \vdash B$

7.2 Exemplos de demonstrações formais em $\mathcal{H}$:

1) É óbvio que, dada uma fbf A num sistema formal, se tem sempre que $A \vdash A$. Então, aplicando do Teorema da Dedução, obtemos o teorema $\vdash A \to A$. A seguir damos uma

demonstração formal deste teorema no sistema de Hilbert, sem recorrer ao Teorema da Dedução:

1. $(A \to ((A \to A) \to)) \to ((A \to (A \to (A \to A)) \to (A \to A))$	H2
2. $A \to ((A \to A) \to))$	H1
3. $((A \to (A \to (A \to A)) \to (A \to A))$	1,2, MP
4. $A \to (A \to A)$	H1
5. $A \to A$	3,4, MP

2) Teorema: $Q \vdash P \to Q$

Prova:

1. Q	premissa
2. $Q \to (P \to Q)$	H1
3. $P \to Q$	1,2, MP

3) Teorema: $A \to B,\ B \to C \vdash A \to C$

Prova (usando a regra T2 provada em 2)):

1. $A \to B$	premissa
2. $B \to C$	premissa
3. $A \to (B \to C)$	2, T2
4. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$	H2
5. $(A \to B) \to (A \to C)$	3, 4, MP
6. $A \to C$	1,3,MP

7.3 Exercícios.

1. Prove as regras seguintes, usando tabelas de verdade.

   (a) Modus ponens (b) $a \to b,\ (\neg a \to b) \models b$

2. Para cada um dos seguintes argumentos, diga quais das regras de inferência dadas na Tabela RI são usadas.

   (a) Se o João esteve na festa de ontem, então faltou à primeira aula da manhã. O João não faltou à primeira aula da manhã. Consequentemente o João não esteve na festa de ontem.

   (b) Se eu fizer isso, serei criticado, e se o não fizer, serei criticado. Consequentemente, serei criticado.

(c) Se está frio e húmido, então é claro que está frio.

(d) Se o Sr. Santos e a Sra. Santos ganham mais de 3 500 contos por ano, a família Santos pode ter férias na Madeira. Como eu sei que o Sr. Santos e a sua esposa ganham mais de 3 500 contos, concluo que a família pode ter férias no Madeira.

(e) Eu sei que a Francisca levou o Fiat ou o Citroen. A Francisca não levou um Citroen. Consequentemente, levou o Fiat.

(f) Se o Quim está em casa então é certo que ele está em casa ou no escritório.

3. Demonstre os seguintes argumentos. Use como regras de inferência apenas o modus ponens, o modus tollens e a lei da combinação. Indique as regras usadas em cada passagem.

   (a) $p,\ p \to (q \vee r),\ (q \vee r) \to s \vdash s$

   (b) $p \to q,\ q \to r,\ \neg r \vdash \neg p$

   (c) $p,\ p \to q \vdash p \wedge q$

4. A demonstração seguinte deduz R das premissas $P \vee Q$, $P \to R$ e $Q \to R$. Falta colocar as justificações dos vários passos. Complete a demonstração, sabendo que para além das regras de inferência da Tabela RI também se usa o $P \vee Q \models (\neg P \to Q)$.

   1. $P \vee Q$
   2. $\neg P \to Q$
   3. $Q \to R$
   4. $\neg P \to R$
   5. $P \to R$
   6. R

5. Dada a premissa $P \wedge Q$, demonstre $P \vee Q$. Use as regras de inferência da simplificação e da adição.

6. Use o Teorema da Dedução para mostrar que $Q \models (P \to Q)$. Use este resultado para mostrar que $\models Q \to (P \to Q)$.

7. Tomando como premissas $P \to Q$, $Q \to R$, e $R \to P$, deduza formalmente $P \leftrightarrow Q$. Use apenas o silogismo hipotético e a lei da introdução da equivalência.

8. Use o Teorema da Dedução e a lei da adição para demonstrar que $\models P \to (P \vee \neg P)$ e $\models \neg P \to (P \vee \neg P)$. Que dedução pode fazer imediatamente de $\models P \to (P \vee \neg P)$ e $\models \neg P \to (P \vee \neg P)$?

9. Considere o sistema natural $\mathcal{L}$.

   (a) Faça uma demonstração formal de $P \wedge Q \equiv Q \wedge P$.

   (b) Demonstre formalmente que $P \to (Q \to R)$ e $P \wedge Q \to R$ são equivalentes.

10. Apresente uma demonstração formal para a equivalência das seguintes proposições:

    (a) Equivalência entre $(p \vee q) \to r$ e $(p \to r) \wedge (q \to r)$

    (b) Equivalência entre $(p \wedge q) \to r$ e $p \to (q \to r)$

11. Considere o sistema formal de Hilbert $\mathcal{H}$.

    (a) Complete a demonstração do teorema $(\neg B \to \neg A) \to (A \to B)$ apresentada a seguir, justificando convenientemente cada passo.
    1. $\neg B \to \neg A$
    2. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$
    3. $A \to (\neg B \to A)$
    4. $(\neg B \to A) \to B$
    5. $A \to B$
    6. $(\neg B \to \neg A) \to (A \to B)$

    (b) Demonstre formalmente os teoremas seguintes:

    (a) $\neg\neg A \to A$ (b) $A \to \neg\neg A$

    (c) $\neg\neg A \equiv A$ (d) $A, B \vdash \neg(A \to \neg B)$ (i.e., A, B $A \wedge B$)

    (e) $(A \to B) \to (\neg B \to \neg A)$ (f) $\neg(A \to \neg B) \vdash B$

8 Algumas considerações sobre a demonstração de implicações

Muitos dos teoremas da Matemática são implicações (ou equivalências, que são conjunções de implicações). Para provar que $P \Rightarrow Q$, ou seja, que de P se deduz Q, ou se quisermos, que $P \to Q$ é tautologia, mostra-se que se P é verdadeira também Q o é. Notemos entretanto que são válidas as seguintes equivalências lógicas:

(1) $p \to q \equiv \neg q \to \neg p$

(2) $p \to q \equiv p \wedge \neg q \to \mathbf{F}$

(A verificação de (1) e (2) fica como exercício.)

As propriedades (1) e (2) proporcionam dois métodos para provar uma afirmação da forma $P \Rightarrow Q$. São eles:

1) Prova indirecta, baseada em (1):

2) Prova por contradição (ou redução ao absurdo), usando (2).

Exemplos

1. Vamos fazer uma demonstração indirecta de que "Se $5n+2$ é ímpar então n é ímpar.":

   Suponhamos que n não é ímpar, ou seja, n é par. Então $5n$ também é par, visto que o produto de um número qualquer por outro par é sempre par. Como a soma de dois pares é par, conclui-se que $5n + 2$ é par, i.e., $5n + 2$ não é ímpar.

2. É bem conhecida a seguinte propriedade:

   (A) "Se $(a_n)_{n\in\mathbf{N}}$ e $(b_n)_{n\in\mathbf{N}}$ são duas sucessões convergentes então a sua soma $(\alpha a_n + \beta b_n)_{n\in\mathbf{N}}$ também é convergente (para quaisquer constantes α e β)."

   Vamos provar por contradição a propriedade seguinte (que é também conhecida):

   (B) "Se $(a_n)_{n\in\mathbf{N}}$ é convergente e $(b_n)_{n\in\mathbf{N}}$ é divergente então a sucessão $(a_n + b_n)_{n\in\mathbf{N}}$ é divergente."

   Demonstração de (B): Sejam $(a_n)_{n\in\mathbf{N}}$ uma sucessão convergente e $(b_n)_{n\in\mathbf{N}}$ uma sucessão divergente . Suponhamos, por contradição, que $(a_n + b_n)_{n\in\mathbf{N}}$ é convergente. Então a sucessão $((a_n + b_n) - a_n)_{n\in\mathbf{N}}$ é convergente, atendendo à propriedade (A). Como $(a_n + b_n) - a_n = b_n$, isto significa que $(b_n)_{n\in\mathbf{N}}$ é convergente, o que contradiz a hipótese. Consequentemente $(a_n + b_n)_{n\in\mathbf{N}}$ tem de ser divergente.

3. Vamos provar que

   $$p \wedge q \to r,\ p,\ \neg r \vdash \neg q$$

   usando prova por contradição. No decorrer da demonstração formal feita a seguir as designações "premissa"e "hipótese"têm dois papéis distintos: As premissas são nete caso $p \wedge q \to r$, p e $\neg r$; chamaremos "hipótese"a uma premissa não dada mas assumida tendo em vista a prova por contradição.

1. $p \wedge q \to r$	premissa
2. p	premissa
3. q	hipótese
4. $p \wedge q$	LC, 2. e 3.
5. r	MP, 1. e 4.
6. $\neg r$	premissa
7. $r \wedge \neg r$	LC, 5. e 6.

Juntando às premissas dadas a negação da conclusão pretendida (ou seja, de $\neg q$), obtivemos a contradição $r \wedge \neg r$. Logo concluimos a veracidade da afirmação $p \wedge q \to r,\, p,\, \neg r \vdash \neg q$.

9 Exercícios

1. Traduza a frase "Uma condição necessária para que o Jorge tenha 14 a Matemática Discreta é ter estudado muito."em cálculo proposicional, usando p com o significado de "O Jorge tem 14 a Matemática Discreta."e q com o significado de "O Jorge estudou muito."

2. Representando "Faz bom tempo"por p, "Vou à praia"por q, "Passo a Matemática Discreta"por r e "Tenho umas boas férias"por s, traduza as duas frases seguintes em cálculo proposicional:

   (a) "Fazer bom tempo é uma condição necessária para eu ir à praia."

   (b) "Passar a Matemática Discreta é condição suficiente para ter umas boas férias."

3. Defina tautologia e mostre que a fórmula bem formada

$$p \vee q \vee r \vee s \vee t \to p \wedge q \wedge r \wedge s \wedge t$$

   não é uma tautologia.

4. Demonstre formalmente que das premissas $p \vee q$, $\neg p$ e $q \to r$ se deduz r.

5. Defina contradição e mostre que a fórmula bem formada

$$(p \to q \wedge r \wedge s) \to p \vee q \vee r \vee t$$

   não é uma contradição.

6. Seja p a proposição "Conduzes a uma velocidade superior a 110."e q a proposição "Apanhas uma multa de velocidade". Traduza as frases seguintes usando p e q e conectivos lógicos.

   (a) Conduzes a uma velocidade superior a 110 mas não apanhas uma multa de velocidade.

   (b) Se não conduzires a uma velocidade superior a 110, não apanhas uma multa de velocidade.

   (c) Conduzires a uma velocidade superior a 110 é condição necessária para apanhares uma multa de velocidade.

7. Faça uma demonstração formal de que das premissas $\neg p \to q \wedge r$, $p \to s$, $\neg s$ se deduz q.

8. Diga se cada uma das implicações é verdadeira ou falsa, justificando sucintamente:

   (a) Se $1 + 1 = 3$ então os cães têm asas.

   (b) Se $1 + 1 = 2$ então os cães têm asas.

9. Seja p a proposição "Vou passar a todas as disciplinas"e q a proposição "Vou fazer férias no Brasil". Traduza as frases seguintes por meio de fórmulas proposicionais.

   (a) Se passar a todas as disciplinas, vou fazer férias no Brasil.

   (b) Para fazer férias no Brasil é necessário e suficiente que passe a todas as disciplinas.

   (c) Se fizer férias no Brasil, passo a todas as disciplinas.

   (d) Vou fazer férias no Brasil só se passar a todas as disciplinas.

   (e) É condição necessária para fazer férias no Brasil que passe a todas as disciplinas.

   (f) Passo a todas as disciplinas ou vou fazer férias no Brasil.

   (g) Ou passo a todas as disciplinas ou não vou fazer férias no Brasil.

10. Averigue se os seguintes argumentos estão correctos, indicando, para cada argumento correcto, a regra de inferência que é usada.

   (a) O número $\log_2 3$ é irracional se não for igual à razão de dois inteiros. Por conseguinte, como $\log_2 3$ não é igual à razão de dois inteiros, conclui-se que $\log_2 3$ é irracional.

(b) Se n é um número real tal que $n > 1$, então $n^2 > 1$. Suponhamos que $n^2 > 1$. Então $n > 1$.

(c) Se n é um número real tal que $n > 3$, então $n^2 > 9$. Suponhamos que $n^2 \leq 9$. Então $n \leq 3$.

(d) A função f tem derivada nula no ponto a ou não tem derivada em a. Como f tem derivada em a, conclui-se que $f'(a) = 0$.

11. (a) Representando as proposições pelas letras indicadas

p : "Durmo menos do que 7 horas por dia." q : "Trabalho muito" r : " Estou cansado"

traduza logicamente as frases seguintes:

i. "Se durmo menos do que 7 horas por dia então trabalho muito."

ii. "Se trabalho muito e durmo menos do que 7 horas por dia então estou cansado."

(b) Quando é que um argumento da forma "De A_1, A_2, ... e A_n deduz-se B"se diz correcto?

(c) Diga, justificando, se o seguinte argumento é ou não correcto: "Se durmo menos do que 7 horas por dia então trabalho muito. Se trabalho muito e durmo menos do que 7 horas por dia então estou cansado. Eu não estou cansado. Logo eu não trabalho muito."

12. Averigue se os seguintes argumentos estão correctos, indicando, para cada argumento correcto, a regra de inferência da Tabela RI que é usada.

(a) O resto da divisão de um número par n por 4 é 0 ou 2. Assim, se o resto da divisão de um número par n por 4 não é 0, então é 2.

(b) Se n é um número primo então é ímpar ou igual a 2. Logo se n é um número par diferente de 2, concluimos que n não é primo.

(c) Se a função f definida por $f(x) = \begin{cases} \frac{e^x+1}{2} & \text{se } x \geq 0 \\ 1 & \text{se } x < 0 \end{cases}$ é diferenciável em todo o $\mathbb{R}$, então é contínua em todo o $\mathbb{R}$. Como a função f é contínua em todo o $\mathbb{R}$, concluimos que f é diferenciável em todo o $\mathbb{R}$.

13. Perante o tribunal compareceram A, B e C, acusados de roubo. Estabeleceu-se que:

Se A não é culpado, culpado é B ou C.

Se A não é culpado então C não é culpado.

Se B é culpado então A é culpado.

Será possível decidir sobre a culpabilidade de A a partir destes factos? Se sim determine se A é ou não culpado.

Capítulo II

Cálculo de Predicados

1 Predicados e quantificadores

Consideremos as afirmações seguintes:

$$x \text{ é par.} \tag{1.1}$$

$$x \text{ é tão alto como } y. \tag{1.2}$$

$$x + y = 0. \tag{1.3}$$

$$x \text{ é pai de } y. \tag{1.4}$$

Denotemos a afirmação (1.1) por $p(x)$. Claro que não faz sentido dizer se $p(x)$ é verdadeira ou falsa. Mas se substituirmos o x por um número natural, já o podemos fazer. Assim $p(2)$ é verdadeira e $p(3)$ é falsa. Analogamente, denotando a afirmação (1.3) por $q(x, y)$, podemos afirmar que $q(1, 2)$ é falsa e $q(-2, 2)$ verdadeira. Também as afirmações (1.2) e (1.4) podem ser tratadas de forma similar atribuindo às variáveis valores num determinado universo de pessoas.

Em geral, uma afirmação envolvendo as variáveis x_1, x_2, ..., x_n pode ser denotada por $p(x_1, x_2, ..., x_n)$; p diz-se um predicado de *aridade* n ou um predicado n*-ário*. Em particular, se $n = 1$, p diz-se unário, se $n = 2$, diz-se binário.

Atentemos agora nas afirmações:

$$\textit{Todo o } x \textit{ é par.} \tag{1.5}$$

$$\textit{Algum } x \textit{ é português.} \tag{1.6}$$

$$\textit{Existe um } x \textit{ tal que } x + x = 0. \tag{1.7}$$

Para expressar estas afirmações podemos usar, para além dos símbolos de predicado, os quantificadores universal e existencial. Usamos $\forall x$ para significar "para todo o x", "todo o x", "para qualquer x, etc. Escrevemos $\exists x$ para expressar de "existe um x", "existe algum x", "existe pelo menos um x", "para algum x", etc. Assim, usando os símbolos de predicado p e q com o significado descrito atrás, podemos representar (1.5) por

$$\forall x\, p(x) \tag{1.8}$$

e (1.7) traduz-se por

$$\exists x\, q(x, x) \tag{1.9}$$

Quanto a (1.6), se representarmos "x é português"por $t(x)$, obtemos

$$\exists x\, t(x) \tag{1.10}$$

Podemos combinar o já aprendido no cálculo proposicional com estes dois novos ingredientes, os predicados e os quantificadores. Por exemplo, sejam as expressões

$$s \to \exists x\, p(x) \tag{1.11}$$

$$p(j) \wedge p(r) \to p(t) \tag{1.12}$$

e tomemos para universo do discurso um certo grupo de pessoas; seja s a proposição "Faz sol", atribuamos a $p(x)$ o significado de "x vai à praia"e sejam j, r e t três pessoas desse grupo, respectivamente, Joana, Rui e Tiago. Deste modo, obtemos para (1.11) a interpretação

"Se faz sol então alguém vai à praia."

e para (1.12) a interpretação

"Se a Joana e o Rui vão à praia então o Tiago também vai à praia."

Exercícios da Secção 1

1. Expresse as seguintes afirmações na forma de cálculo de predicados. O domínio considerado é o conjunto dos números inteiros.

   (a) Se x está entre 1 e 2, e se y está entre 2 e 3, então a diferença entre x e y não pode exceder 2. Use o predicado $b(x, y, z)$ se x está entre y e z, e use $d(x, y, z)$ se a diferença entre x e y é maior do que z.

   (b) Se x é divisível por quatro então x não pode ser primo. Use $d(x, y)$ se x é divisível por y e $p(x)$ se x é primo.

   (c) $x + y = z$ e $x + z = u$. Use $s(x, y, z)$ se $x + y = z$.

2. Suponha que o universo de discurso é um grupo de pessoas. Traduza a afirmação "Toda a gente aqui fala inglês ou francês."em cálculo de predicados.

3. Expresse ”Nenhum número natural é negativo.”supondo que o universo do discurso é

   (a) o conjunto dos números naturais;

   (b) o conjunto dos números inteiros;

   (c) o conjunto dos números reais.

4. No domínio de todos os animais como traduziria as seguintes expressões em cálculo de predicados?

   (a) Todos os leões são predadores.
   (b) Alguns leões vivem em África.
   (c) Só os leões rugem.
   (d) Alguns animais comem insectos.
   (e) As aranhas comem insectos.
   (f) As aranhas só comem insectos.

5. No domínio dos números naturais escreva simbolicamente as seguintes expressões usando $p(x)$ para ”x é primo”e $q(x)$ para ”x é par”. Pode usar também $x < y$ para cada x e y.

   (a) Alguns primos são pares.

   (b) Todos os números pares são maiores do que 1.

   (c) Um número par é primo se e só se for menor que 3.

   (d) Não existem números primos menores que 3.

2 Fórmulas bem formadas

Expressões como as (1.8), (1.9), (1.10), (1.11) e (1.12) são exemplos de fórmulas bem formadas do cálculo de predicados, que vamos definir a seguir.

Símbolos do Cálculo de Predicados:

Variáveis: x, y, z, ...
Constantes: a, b, c, ...
Símbolos de predicado: p, q, r, ...
Conectivos: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
Quantificadores: $\forall$, $\exists$
Auxiliares: ( )

Chama-se *termo* a toda a variável ou constante.

Um *predicado atómico* é toda a expressão do tipo $p(t_1, t_2, ..., t_n)$ onde p é um símbolo de predicado de aridade n e $t_1, t_2, ..., t_n$ são termos; **V**, **F** e todo símbolo proposicional são também predicados atómicos.

Fórmulas bem formadas (fbf)

- Todo o predicado atómico é uma fórmula bem formada;
- Se A e B são fbf's e x é uma variável, então as expressões seguintes são fórmulas bem formadas:

  (A), $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$, $\exists x\, A$ e $\forall x\, A$

Prioridade dos conectivos e quantificadores:

$$\neg,\ \exists x,\ \forall y$$

$$\wedge$$

$$\vee$$

$$\rightarrow$$

Escopo de um quantificador:

Na fbf $\exists x\, A$, A diz-se o escopo do quantificador $\exists x$.
Na fbf $\forall x\, A$, A é o escopo do quantificador $\forall x$.

Exemplo: O escopo de $\exists x$ na fbf

$$\exists x\, p(x,y) \rightarrow q(x) \tag{2.1}$$

é $p(x,y)$. O escopo de $\exists x$ na fbf

$$\exists x\, (p(x,y) \rightarrow q(x)) \tag{2.2}$$

é $p(x,y) \rightarrow q(x)$.

A ocorrência de uma variável x numa fbf diz-se *limitada* se ela figurar num quantificador ou estiver no escopo de $\exists x$ ou de $\forall x$. Caso contrário, diz-se *livre* ou *muda*. Por exemplo, as duas primeiras ocorrências de x em (2.1) são limitadas, a última ocorrência de x é livre e a única ocorrência de y é livre. Em (2.2), todas as ocorrências de x são limitadas.

Exercícios da Secção 2

1. Determine as variáveis livres e as limitadas em $(\forall x \exists y p(x, y, z) \wedge q(y, z)) \wedge r(x)$.

2. Escreva uma fbf do cálculo de predicados que contenha um quantificador existencial, um quantificador universal, dois símbolos de predicado, A e B, o primeiro de aridade 2, segundo de aridade 1, a ocorrência da variável x duas vezes, ambas limitadas, a ocorrência da variável y três vezes, duas limitadas e uma livre.

3 Semântica

Interpretações

Na primeira secção interpretámos algumas fbf's do cálculo de predicados. Vamos precisar o significado de interpretação de uma fbf.

Uma *interpretação* para uma fbf consiste em:

- Um conjunto não vazio D, chamado *domínio* ou *universo* da interpretação, juntamente com uma correspondência que associa os símbolos da fbf com elementos de D do seguinte modo:

- A cada símbolo de predicado corresponde uma determinada relação entre elementos de D. Um predicado sem argumentos é uma proposição e atribui-se-lhe um dos valores V ou F.

- A cada variável livre faz-se corresponder um elemento de D. A todas as ocorrências livres de uma mesma variável faz-se corresponder o mesmo elemento de D.

- A cada constante faz-se corresponder um elemento de D. A todas as ocorrências de uma mesma constante faz-se corresponder o mesmo elemento de D.

Exemplo Uma interpretação possível para a fbf

$$\exists x \, \forall y \, (q(x, y) \rightarrow q(y, z)) \tag{3.1}$$

é:

Universo: alunos de uma dada escola;
$q(x, y) :=$ "x é amigo y."
$z := c$, onde c representa uma determinada pessoa chamada Carlos.

Deste modo, o significado de (3.1) é: "Existe um aluno tal que aqueles de quem ele é amigo são amigos de Carlos."

Uma outra interpretação para a mesma fbf:

$$\begin{aligned}&\text{Universo: } \mathbb{R}\\&q(x,y) := x \times y = 0\\&z := 2\end{aligned} \tag{3.2}$$

Com a segunda interpretação obtemos uma proposição verdadeira. Na verdade, seja $x = 1$. Então, se $q(x,y)$ for verdadeira, temos $1 \times y = 0$, pelo que tem de ser $y = 0$ e, consequentemente, $y \times y = 2$; ou seja, $q(y,a)$ é verdadeira. Portanto, a implicação $q(1,y) \to q(y,2)$ é verdadeira para todo o y. Havendo um x que torna a implicação $q(x,y) \to q(y,2)$ verdadeira, concluimos que $\exists x\, \forall y\, (q(x,y) \to q(y,z))$ é verdadeira para esta interpretação.

Seja A uma fbf, x uma variável e t um termo. Então

$$S_t^x A$$

representa a expressão obtida substituindo todas as ocorrências de x por t.

Uma fbf diz-se uma *variante de* $\forall x\, A$ se for da forma $\forall y\ S_y^x A$ onde y é uma variável. Analogamente, $\exists x\, A$ e $\exists y\, S_y^x A$ são *variantes* uma da outra.

Validade

Uma fbf do cálculo dos predicados diz-se:

válida ou uma *tautologia*,	se for verdadeira para todas as possíveis interpretações;
satisfazível,	se existirem interpretações para as quais ela é verdadeira;
contraditória ou uma *contradição*,	se for falsa para qualquer interpretação.

Se A é uma fbf válida, escrevemos $\models A$.

Se B é uma fbf, então toda a interpretação que torna B verdadeira diz-se *satisfazer* B. Toda a interpretação que satisfaz B diz-se *modelo de* B.

Exemplo A interpretação (3.2) é um modelo de (3.1). Fica como exercício arranjar uma interpretação de (3.1) que a torne falsa e concluir que, portanto, (3.1) não é uma tautologia.

Exercícios da Secção 3

1. Expresse sob a forma de predicados $S^x_3\, p(x,y)$, $S^x_y\, p(x,y)$, $S^x_y\,(p(x) \wedge \forall x q(x))$ e $S^y_2\,(p(x) \wedge q(y) \wedge r(x,y))$.

2. Um universo contém três indivíduos a, b e c. Para estes indivíduos, define-se um predicado $q(x,y)$, cujos valores lógicos são dados pelo quadro seguinte:

	a	b	c
a	V	F	V
b	F	V	V
c	F	V	V

   Estude a veracidade de:

   (i) $\forall x \exists y\, q(x,y)$ (ii) $\forall y\, q(y,b)$ (iii) $\forall y\, q(y,y)$ (iv) $\exists x\, \neg q(a,x)$

   (v) $\forall y\, q(b,y)$ (vi) $\forall y\, q(y,y) \wedge \forall x \exists y\, q(x,y)$.

3. Um universo de discurso consiste em três pessoas, nomeadamente, João, Maria e Joana. Os três são estudantes, e nenhum deles é rico. Os símbolos de predicados e, h, m e r correspondem a ser estudante, ser homem, ser mulher e ser rico, respectivamente.

   (a) Para cada uma das expressões seguintes, diga se é verdadeira ou falsa: $\forall x\, e(x)$, $\forall x\, m(x) \vee \forall x\, h(x)$, $\forall x\,(m(x) \vee h(x))$, $\exists x\, r(x)$ e $\exists x\,(m(x) \to r(x))$.

   (b) Supondo p verdadeiro e q falso, determine $\forall x\, p$, $\forall x\, q$, $\exists x\,(p \wedge m(x))$, $\exists x\,(p \vee m(x))$ e $\exists x(q \vee m(x))$.

4. Será que a expressão $p(x) \to (p(x) \vee q(x))$ é válida? Justifique.

5. Numa certa interpretação o domínio consiste nos indivíduos a, b e c, e existe um predicado p de aridade 2 tal que $p(x,x)$ é verdadeiro para todos os possíveis valores de x, $p(a,c)$ é verdadeiro e $p(x,y)$ é falso para todos os outros casos em que x é diferente de y. Determine o valor lógico de

   (a) $p(a,b) \wedge p(a,c)$ (b) $p(c,b) \vee p(a,c)$ (c) $p(b,b) \wedge p(c,c)$ (d) $p(c,a) \to p(c,c)$

6. Seja A a expressão $(p(x) \to q(y)) \wedge \neg q(y) \wedge p(y)$.

   (a) Determine um modelo para A.

   (b) Comente a seguinte afirmação: "A expressão $\forall x \forall y A$ é uma contradição."

7. Mostre que $(p(x) \to q(y)) \wedge (q(y) \to r(z)) \to (p(z) \to q(z))$ não é válida.

4 Fórmulas equivalentes

Duas fbf's A e B dizem-se *logicamente equivalentes* se $A \leftrightarrow B$ for válida. Neste caso, escrevemos

$$A \equiv B$$

Segue-se uma tabela com algumas equivalências básicas.

Equivalências básicas no cálculo de predicados:

1. $\forall x\, A \equiv A$ se x não for livre em A
2. $\exists x\, A \equiv A$ se x não for livre em A
3. $\forall x\, A \equiv \forall y\, S_y^x A$ se y não for livre em A
4. $\exists x\, A \equiv \exists y\, S_y^x A$ se y não for livre em A
5. $\forall x\, A \equiv S_t^x A \wedge \forall x\, A$ para todo o termo t
6. $\exists x\, A \equiv S_t^x A \vee \exists x\, A$ para todo o termo t
7. $\forall x\, (A \vee B) \equiv A \vee \forall x\, B$ se x não for livre em A
8. $\exists x\, (A \wedge B) \equiv A \wedge \exists x\, B$ se x não for livre em A
9. $\forall x\, (A \wedge B) \equiv \forall x\, A \wedge \forall x\, B$
10. $\exists x\, (A \vee B) \equiv \exists x\, A \vee \exists x\, B$
11. $\forall x \forall y\, A \equiv \forall y \forall x\, A$
12. $\exists x \exists y\, A \equiv \exists y \exists x\, A$
13. $\neg\exists x\, A \equiv \forall x\, \neg A$
14. $\neg\forall x\, A \equiv \exists x\, \neg A$

Vamos provar e comentar algumas das equivalências. A prova das restantes fica como exercício.

1. Queremos mostrar que $\forall x\, A \leftrightarrow A$ é uma tautologia. Como x não é livre em A, seja qual for a interpretação que considerarmos, a veracidade de A é independente do x que figura no quantificador $\forall x$. Logo A é verdadeira se e só se $\forall x\, A$ o for, ou seja, $\forall x\, A$ e A vão ter sempre o mesmo valor lógico.

Exemplos de aplicação da propriedade 1: $\forall x\, \exists y\, p(y) \equiv \exists y\, p(y)$, $\forall x\, q(y,z) \equiv q(y,z)$.

Mas é claro que $\forall x\, \exists y\, r(x,y) \not\equiv \exists y\, r(x,y)$. (Porquê?)

5. Dado um determinado universo, $\forall x\, A$ é verdadeira se e só se A é verdadeira para toda a concretização de x nesse universo. Então, em particular, A é verdadeira para $x := t$. Como a conjunção de duas proposições verdadeiras é verdadeira, conclui-se que $S_t^x A \wedge \forall x\, A$ é verdadeira. Reciprocamente, se $S_t^x A \wedge \forall x\, A$ é verdadeira então, por definição da conjunção, $\forall x\, A$ tem de ser verdadeira.

Exemplo: $\forall x \exists y\, s(x,y) \equiv \exists y\, s(z,y) \,\wedge\, \forall x \exists y\, s(x,y)$.

8. Se existe um elemento x do universo tal que $A \wedge B$ é verdadeira para esse x então A e B são verdadeiras para esse x. Mas, como x não é livre em A, a veracidade de A não depende de x, logo $A \wedge \exists x\, B$ é também verdadeira. Reciprocamente, se $A \wedge \exists x\, B$ é verdadeira, temos que A é verdadeira independentemente de x e B é verdadeira para um certo x, logo $A \wedge B$ é verdadeira para esse x e, portanto, verifica-se que $\exists x\, (A \wedge B)$.

Exemplo: $\exists x\, (p(z) \wedge q(x)) \equiv p(z) \wedge \exists x\, q(x)$.

Mas $\exists x\, (p(x) \wedge q(x)) \not\equiv p(x) \wedge \exists x\, q(x)$.

As propriedades 13 e 14 são as *Leis de De Morgan* para os quantificadores. A sua prova fica também como exercício. Notemos entretanto que, quando nos situamos num universo finito $U = \{a_1, a_2, ..., a_n\}$, temos que:

- A fbf $\forall x\, p(x)$ representa uma conjunção de proposições, pois se tem

$$\forall x\, p(x) \equiv p(a_1) \wedge p(a_a) \wedge ... \wedge p(a_n)\,.$$

- A fbf $\exists x\, p(x)$ representa uma disjunção de proposições, verificando-se

$$\exists x\, p(x) \equiv p(a_1) \vee p(a_a) \vee ... \vee p(a_n)\,.$$

Aplicando as Leis de De Morgan (generalizadas) a cada um dos casos temos:

$$\neg\, \forall x\, p(x) \equiv \neg(p(a_1) \wedge p(a_a) \wedge ... \wedge p(a_n)) \equiv \neg p(a_1) \vee \neg p(a_2) \vee ... \vee \neg p(a_n) \equiv \exists x\, \neg p(x)$$

$$\neg\, \exists x\, p(x) \equiv \neg(p(a_1) \vee p(a_2) \vee ... \vee p(a_n)) \equiv \neg p(a_1) \wedge \neg p(a_2) \wedge ... \wedge \neg p(a_n) \equiv \forall x\, \neg p(x)$$

Exercícios da Secção 4

1. Use as equivalências lógicas básicas estudadas na aula teórica e as leis de comutatividade do cálculo proposicional para provar as equivalências lógicas seguintes. Suponha que x não ocorre livremente em A.

   (a) $(\exists x\, B) \wedge A \equiv \exists x(B \wedge A)$

   (b) $(\forall x\, B) \wedge A \equiv \forall x(B \wedge A)$

2. Em cada um dos casos seguintes, mova todos os quantificadores para o início da expressão de forma a obter uma expressão logicamente equivalente.

   (a) $\forall x\, p(x) \vee \forall x(q(x) \to p(x))$

   (b) $\exists x\, p(x) \wedge \exists x(q(x) \wedge p(x))$.

3. Suponha que $f(x)$ representa "x encontra um erro"e que q representa "o erro do programa pode ser corrigido". Traduza

$$\forall x(f(x) \to q).$$

4. Suponha que P representa a expressão $\exists y\, r(y)$. Use as regras básicas sobre equivalências lógicas estudadas na aula teórica para mostrar que

$$\exists x(P \vee q(x)) \equiv \exists x \exists y(q(x) \vee r(y)).$$

5 Argumentos correctos

Consideremos os seguintes argumentos:

1. Todos os gatos têm garras.
2. Tom é um gato.

---

3. Tom tem garras.

1. $\forall x\,(g(x) \to r(x))$
2. $g(t)$

---

3. $r(t)$

---

1. Toda a gente fala francês ou inglês.
2. A Joana não fala inglês.

---

3. A Joana fala francês.

1. $\forall x\,(i(x) \vee f(x))$
2. $\neg i(j)$

---

3. $f(j)$

Ambos os argumentos estão correctos. Analisemos por exemplo o primeiro: Se $\forall x\,(g(x) \to r(x))$ se verifica então $g(x) \to r(x)$ verifica-se para todo o x, em particular $g(t) \to r(t)$ é verdadeira. Como $g(t)$ se verifica, usando Modus Ponens concluimos $r(t)$.

Tal como no cálculo proposicional, no cálculo de predicados também escrevemos

$$A_1,\, A_2,\, ...\, A_n \models B$$

para afirmar que o argumento " De A_1, A_2, ..., A_n deduz-se B"é correcto, ou seja, que $A_1 \wedge A_2 \wedge ... \wedge A_n \to B$ é válida.

Exercícios da Secção 5

1. Averigue se cada um dos argumentos seguintes é ou não correcto:

   (a) $\forall x\, p(x),\, \forall x\, q(x) \models \forall x\,(p(x) \wedge q(x))$

   (b) $\exists x\, p(x) \models \forall x\, p(x)$

(c) $\exists x\, p(x),\ \forall x\, (p(x) \to q(x)) \models \forall x\, q(x)$

2. Formalize os seguintes argumentos e diga se são ou não correctos.

   (a) Há aqui alguém que fala inglês e francês. Logo há aqui alguém que fala inglês e há aqui alguém que fala francês.

   (b) Todas as pessoas aqui presentes falam francês ou inglês. Logo todas as pessoas aqui presentes falam francês ou todas falam inglês.

6 Sistema formal para o Cálculo de Predicados

O sistema formal que vamos considerar para o cálculo dos predicados é constituído por:

1. Símbolos:

   $\neg,\ \wedge,\ \vee,\ \to, \leftrightarrow,\ \forall,\ \exists$

   parêntesis (e)

   variáveis x, y, z, ...

   constantes

   símbolos de predicado

2. Fórmulas bem formadas: como definido atrás.

3. Regras de inferência

   - Todas as da Tabela RI
   - Regras de inferência para o quantificador universal
   - Regras de inferência para o quantificador existencial

4. Teorema da Dedução

O sistema formal acabado de descrever é completo e correcto, ou seja, verifica-se $A_1,\ A_2,\ ...,\ A_n \models B$ se e só quando se verificar $A_1,\ A_2,\ ...,\ A_n \vdash B$. Dito doutro modo, $A_1 \wedge A_2 \wedge ... \wedge A_n \to B$ é uma tautologia se e só se, dentro deste sistema formal, das premissas $A_1,\ A_2,\ ...,\ A_n$ se deduz B.

Como mencionado, este sistema tem novas regras de inferência que respeitam aos quantificadores. Vamos descrevê-las a seguir.

Regras de inferência para os quantificadores universal e existencial

Eliminação universal (EU)

A *eliminação do quantificador universal*, abreviadamente *Eliminação Universal*, é uma regra de inferência que estabelece que da premissa $\forall x\, A(x)$ se deduz que $A(t)$ é verdadeira para todo o elemento t do universo de discurso. Abreviadamente:

$$\frac{\forall x\, A}{S_t^x A}$$

Por exemplo, de $\forall x\, p(x, y)$ deduz-se $p(z, y)$, onde z representa um qualquer elemento do universo. Também por EU, se infere $p(x, y)$ de $\forall x\, p(x, y)$. Outro exemplo: De $\forall x\, \exists y\, q(x, y)$ deduz-se $\exists y\, q(x, y)$; mas atenção, de $\forall x\, \exists y\, q(x, y)$ não se pode inferir $\exists y\, q(y, y)$: é claro que o x que torna $q(x, y)$ verdadeira não tem de ser o próprio y.

Temos pois de respeitar algumas normas quando usamos a Eliminação Universal, nomeadamente:

De uma fbf da forma $\forall x\, A$, podemos inferir uma fbf aplicando S_t^x a A, se t for livre para substituir x em A, i.e., se não existirem ocorrências x em A no escopo de algum quantificador que limite t.

Por exemplo:
A variável x é sempre livre para substituir x em $A(x)$.
Toda a constante é sempre livre para substiuir x em $A(x)$.
Se y não ocorre em $A(x)$, y é livre para substiuir x em $A(x)$.

Exemplos:

1. Demonstração formal de $\forall x(h(x) \to m(x)), h(s) \vdash m(s)$:

1. $\forall x(h(x) \to m(x))$	premissa
2. $h(s)$	premissa
3. $h(s) \to m(s)$	1. e EU (S_s^x)
4. $m(s)$	2., 3. e MP

   Uma interpretação:

   1. Todos os humanos são mortais.
   2. Sócrates é um humano.
   3. Sócrates é mortal.

2. Demonstração formal de

   $\forall x(f(d,x) \to s(x,d) \vee r(x,d)),\ f(d,p),\ \neg r(p,d) \vdash s(p,d)$:

1. $\forall x(f(d,x) \to s(x,d) \vee r(x,d))$	premissa
2. $f(d,p)$	premissa
3. $\neg r(p,d)$	premissa
4. $f(d,p) \to s(p,d) \vee r(p,d)$	1. e EU(S_p^x)
5. $s(p,d) \vee r(p,d)$	2., 4., e MP
6. $s(p,d)$	3., 5. e SD

   (Exercício: Arranje uma interpretação para este caso.)

Eliminação existencial (EE)

A *eliminação do quantificador existencial*, abreviadamente *Eliminação Existencial*, é uma regra de inferência que estabelece que da premissa $\exists x\, A(x)$ se deduz $A(b)$, onde b é uma nova constante na prova. Abreviadamente:

$$\frac{\exists x\, A}{S_b^x A}$$

Exemplo: Vamos demonstrar que

$$\forall x \neg p(x) \vdash \neg \exists x p(x)\,.$$

Na demonstração vamos usar *prova por contradição* que, como vimos atrás, consiste em assumir as premissas juntamente com a negação da tese chegando assim a uma contradição.

1. $\exists x\, p(x)$	hipótese (por contradição)
2. $p(b)$	1. e EE
3. $\forall x\, \neg p(x)$	premissa
4. $\neg p(b)$	3. e EU
5. $p(b) \wedge \neg p(b)$	2., 4. e LC
6. F	5. (porque $A \wedge \neg A \vdash F$)

Conclui-se $\forall x \neg p(x) \vdash \neg \exists x p(x)$, de 1., 3. e 6., por contradição.

Introdução universal (IU)

A *introdução do quantificador universal*, abreviadamente *Introção Universal*, é uma regra de inferência que estabelece que da premissa de que $A(t)$ é verificada para todo o membro do universo do discurso se deduz $\forall x\, A(x)$. Abreviadamente:

$$\frac{S^x_t A}{\forall x\, A}$$

Esta regra de inferência só pode ser usada com limitações adequadas, nomeadamente:

De A deduz-se $\forall x\, A$ se x não é *variável pendente* nem *variável subescrita* em A.

Antes de nos debruçarmos sobre os conceitos de variável pendente ou subescrita, seguem-se dois exemplos de demonstração formal onde é usada Introdução Universal. Note-se que em todos os casos esta regra de inferência foi aplicada nas condições seguintes: tem-se uma fbf A onde figura uma certa variável w que representa qualquer membro do universo de discurso e aplica-se o quantificador universal afectado por uma variável z a $S^w_z A$.

Exemplos:

1. Demonstração formal de $\forall x\, P(x)$, $\forall x(P(x) \to Q(x)) \vdash \forall x Q(x)$:

1. $\forall x P(x)$	premissa
2. $\forall x(P(x) \to Q(x)$	premissa
3. $P(x)$	1., e EU(S^x_x)
4. $P(x) \to Q(x)$	2. e EU(S^x_x)
5. $Q(x)$	3., 4. e MP
6. $\forall x Q(x)$	5. e IU

2. Demonstração formal de $\forall x \forall y P(x, y) \vdash \forall y \forall x P(x, y)$:

1. $\forall x \forall y P(x, y)$	premissa
2. $\forall y P(x, y)$	1. e EU(S^x_x)
3. $P(x, y)$	2. e EU(S^y_y)
4. $\forall x P(x, y)$	3. e IU
5. $\forall y \forall x P(x, y)$	4. e IU

De forma a compreender as restrições que se impõem na aplicação da Introdução Universal, e que justificam as definições de variável pendente e variável subescrita, consideremos alguns exemplos:

1) É claro que da premissa $p(x)$ não podemos deduzir $\forall x\, p(x)$. Na verdade é fácil arranjar uma interpretação que torne $p(x)$ verdadeira e $\forall x\, p(x)$ falsa. Basta considerar

$\mathbb{N}$ como universo, $p(x) :=$*x é um primo diferente de dois.* e atribuir à variável livre x o valor 3; então $p(3)$ é verdadeira mas $\forall x\, p(x)$ é falsa.

2) Suponhamos que temos a seguinte sequência de fbf's:

1. $p(x)$	premissa
2. $\forall x\,(p(x) \to q(x))$	premissa
3. $p(x) \to q(x)$	2. e EU
4. $q(x)$	1., 3. e MP

Se aplicássemos a seguir o quantificador universal, acrescentando uma quinta linha

5. $\forall x\, q(x)$

a prova formal ficaria incorrecta. Na verdade, adoptando a interpretação usada em 1) juntamente com $q(x) :=$ *x é ímpar.*, vem que as premissas $p(x)$ e $\forall x\,(p(x) \to q(x))$ são verdadeiras mas $\forall x\, q(x)$ é obviamente falsa. (Justifique.)

Mais uma vez o problema decorreu do facto de x ser uma variável livre numa premissa, premissa essa que se usa em 3.

3) Seja a sequência de fbf's

1. $\exists x\, p(x)$	premissa
3. $p(x)$	1. e EE

É evidente que de 3. não podemos deduzir $\forall x\, p(x)$, pois é fácil arranjar um exemplo de interpretação que torne $\exists x\, p(x)$ verdadeira e $\forall x\, p(x)$ falsa.

4) Um outro exemplo envolvendo EE:

1. $\forall x\, \forall y\, p(x,y)$	premissa
2. $\forall x\, \exists y\, ((p(x,y) \to q(x,y))$	premissa
3. $\forall y\, p(x,y)$	1. e EU
4. $p(x,y)$	3. e EU
5. $\exists y\, ((p(x,y) \to q(x,y))$	2. e EU
6. $p(x,y) \to q(x,y)$	5. e EE
7. $q(x,y)$	4., 6. e MP

Neste caso também não podemos aplicar Introdução Universal à fbf de 7. Se o fizessemos estaríamos a inferir $\forall x\, q(x,y)$ das premissas $\forall x\, \forall y\, p(x,y)$ e $\forall x\, \exists y\, ((p(x,y) \to q(x,y))$. Mas isso é incorrecto como se pode ver através da seguinte interpretação:

universo: $\mathbb{N}$
$p(x,y) := x + y \geq 0$
$q(x,y) := x \leq y$

De acordo com este quadro, temos que:

– As premissas são verdadeiras. A premissa $\forall x\,\forall y\,p(x,y)$ é verdadeira, visto que significa que a soma de quaisquer dois números naturais é maior ou igual a zero. Quanto à veracidade da premissa $\forall x\,\exists y\,((p(x,y) \rightarrow q(x,y))$: Para ela ser verdadeira tem de $\exists y\,((p(x,y) \rightarrow q(x,y))$ ser verdadeira para todo o natural x; isto verifica-se pois, como $q(x,x)$ é verdadeira para todo o x, conclui-se que, escolhendo, para cada natural x, $y := x$, a implicação $p(x,y) \rightarrow q(x,y)$ fica verdadeira.

Mas

– $\forall x\,q(x,y)$, que significa que todo o natural x é menor ou igual que um determinado y, é obviamente falsa.

Nos exemplos anteriores aparecem variáveis pendentes e subescritas, de acordo com as definições que se seguem.

Uma *variável pendente* define-se recursivamente do seguinte modo:

• Uma variável x numa fbf A é uma *variável pendente em* A se x é livre em A e A é uma premissa.

• Uma variável x numa fbf A é uma *variável pendente em* A se A é inferida de uma fbf na qual x é uma variável pendente.

Um exemplo:

1. $p(x)$	premissa	x é pendente
2. $\forall x\,q(x)$	premissa	
3. $q(x)$	2. e EU	
4. $p(x) \wedge q(x)$	1., 3. e LC	x é pendente

Nos exemplos 1) e 2) tinhamos também uma variável pendente que impedia a aplicação de IU. (Verifique.)

Uma *variável subescrita* define-se recursivamente do seguinte modo:

• Uma variável x numa fbf A diz-se uma *variável subescrita em* A se x é livre em A e existe uma constante b em A que foi criada pela regra EE.

• Uma variável x numa fbf A é uma *variável subescrita em* A se A é inferida de uma fbf na qual x é uma variável subescrita.

Exemplo:

1. $\forall x \exists y\, p(x,y)$	premissa	
2. $\exists y\, p(x,y)$	1. e EU	
3. $p(x,c)$	2. e EE	x é subescrita
4. $p(x,c) \vee q(x,y)$	1., 3. e LA	x é subescrita

Nos exemplos 3) e 4) foi também a presença de uma variável subescrita que não permitiu o uso de Introdução Universal. (Verifique.)

Seguem-se mais dois exemplos de demonstrações formais onde se faz uso de IU.

Exemplos:

1. Teorema: $\forall x P(x) \vdash \forall y P(y)$

   Prova:

1. $\forall x P(x)$	premissa
2. $P(y)$	1. e EU(S_y^x)
3. $\forall y P(y)$	2. e IU

2. Um exemplo em que se usa o Teorema da Dedução:

   Teorema: $\forall x(s(x) \to p(x)) \vdash \forall x(\neg p(x) \to \neg s(x))$

   Prova:

1. $\forall x(s(x) \to p(x))$	premissa
2. $s(x) \to p(x)$	1. e EU(S_x^x)
3. $\neg p(x)$	hipótese
4. $\neg s(x)$	2., 3. e MT
5. $\neg p(x) \to \neg s(x)$	3., 4.9 e TD
6. $\forall x(\neg p(x) \to \neg s(x))$	5. e IU

Introdução existencial (IE)

A *introdução do quantificador existencial*, abreviadamente *Introdução Existencial*, é uma regra de inferência que estabelece que da premissa de que $A(t)$ se verifica para algum membro t do universo de discurso se deduz $\exists x\, A(x)$. Abreviadamente:

$$\frac{S_t^x A}{\exists x\, A}$$

Mais precisamente:

De $S_t^x A$ infere-se $\exists x A$ se t for livre para substituir x em A, i.e., se não existirem ocorrências x em A no escopo de algum quantificador que limite t.

(Note-se que, por definição, assumimos que todo o universo é não vazio.)

Exercício: Dê um exemplo de aplicação indevida de Introdução Existencial, justificando com uma interpretação adequada.

Exemplo: Demonstração de $\forall x(w(x) \to r(x))$, $w(m) \vdash \exists x r(x)$:

1. $\forall x(w(x) \to r(x))$	premissa
2. $w(m) \to r(m)$	1. e EU (S_m^x)
3. $w(m)$	premissa
4. $r(m)$	2., 3. e MP
5. $\exists x r(x)$	4. e IE

Exercícios da Secção 6

1. Dados P e $\forall x(P \to Q(x))$, construa uma demonstração formal para $\forall x\, Q(x)$. Como regras de inferência, use eliminação universal, introdução universal e modus ponens.

2. Dados $\forall x \neg q(x)$ e $\forall x(p(x) \to q(x))$, dê uma demonstração formal de $\forall x \neg p(x)$. Use eliminação universal, introdução universal e modus tollens como regras de inferência.

3. Faça uma demonstração formal para mostrar que $\exists x \exists y\, a(x, y)$ implica logicamente $\exists y \exists x\, a(x, y)$. Use eliminação existencial e introdução existencial como regras de inferência.

4. Demonstre formalmente que $\forall x A(x)$ implica formalmente que $\exists x A(x)$.

5. Suponha que $f(x, y)$ denota o facto de x ser filho de y, e que $p(x, y)$ denota o facto de y ser um dos pais de x. Então é claro que

   $$\forall x \forall y(f(x, y) \to p(x, y))$$

   Faça uma demonstração formal para mostrar que se Pedro é filho de Joana, então Joana é um dos pais de Pedro.

6. Se $v(x, y)$ designa o facto de x e y viverem na mesma cidade, então temos que

   $$\forall x \forall y \forall z(v(x, y) \wedge v(y, z) \to v(x, z))$$

   Usando-o como uma das premissas, dê uma demonstração formal de que se Pedro vive na mesma cidade que Maria, e Maria vive na mesma cidade que Bruno, então Pedro vive na mesma cidade que Bruno.

7 Regras para a igualdade

As interpretações de um predicado binário $p(x, y)$ podem ser de vários tipos. Por exemplo,

$p(x, y) :=$ "x é filho de y"
$p(x, y) := x \geq y$
$p(x, y) :=$ "x e y pertencem à mesma espécie"

Claro que cada uma destas interpretações só faz sentido num universo adequado. Assim a primeira pode dizer respeito a um grupo de pessoas, a segunda a um conjunto de números e a terceira a um grupo de animais. Mas a atribuição

$$p(x, y) := (x = y)$$

tem sentido em qualquer universo que se considere. Daí o ser comum usar o predicado binário da igualdade em fbf's do cálculo de predicados exactamente na forma $x = y$. Deste modo, por exemplo, a expressão

$$\forall x\, \exists y\, (x = y) \tag{7.1}$$

é uma fórmula bem formada. Outro exemplo de fbf contendo o predicado igualdade:

$$\exists y\, \forall x\, (x = y) \tag{7.2}$$

Exercício: Mostre que (7.1) é válida mas (7.2) o não é. Será (7.2) contraditória? Justifique.

A igualdade é um predicado com que lidamos amiúde no dia a dia matemático, e cujas características conhecemos bem. A seguir explicitam-se propriedades essenciais relativas à igualdade.

Introdução da igualdade
(Qualquer coisa é igual a si própria)

$$t = t$$

Lei da existência
(Os domínios interpretativos são sempre não vazios)

$$\vdash\ \exists x\, (x = x)$$

Eliminação da igualdade
(Coisas iguais têm as mesmas propriedades)

$$t_l = t_2,\ \phi(t_1)\ \vdash\ \phi(t_2)$$

Propriedades da igualdade

$\vdash \forall x(x = x)$	(reflexividade)	
$\vdash \forall x \forall y(x = y \to y = x)$	(simetria)	$\dfrac{s = t}{t = s}$
$\vdash \forall x \forall y \forall z(x = y \wedge y = z \to x = z)$	(transitividade)	$\dfrac{r = s,\ s = t}{r = t}$

Igualdade e unicidade

Enquanto o quantificador $\exists$ significa "existe pelo menos um", o símbolo $\exists^1$ (ou $\exists!$) usa-se com o significado de " Existe um e um só". Portanto $\exists^1 x$ refere-se não só à existência de um x mas também à sua unicidade. Põe-se a questão: Como traduzir em cálculo de predicados (só com o uso dos quantificadores $\forall$ ou $\exists$) uma afirmação do tipo $\exists^1 x\, p(x)$? Dão-se a seguir duas formas de expressar $\exists^1 x\, p(x)$. Fica como exercício a verificação de que elas estão correctas.

$$\exists^1 x\, p(x) \equiv \exists x(p(x) \wedge \forall y(p(y) \to (y = x))$$

$$\exists^1 x p(x) \equiv \exists x p(x) \wedge \forall x \forall y(p(x) \wedge p(y) \to (x = y))$$

Exercícios da Secção 7

1. Use as regras de inferência da igualdade para mostrar que

$$(x = y) \wedge (y \leq z) \to (x \leq z).$$

2. Considere $e(x)$: x é um electricista, e seja j o representante de João. Expresse simbolicamente "João é o único electricista"com e sem o símbolo $\exists^1$.

3. Suponhamos que $f(x) = y$ se $x = y^2$ e consideremos a seguinte "demonstração formal"

   1. $1 = 1$ reflectividade da igualdade

   2. $1 = f(1)$ definição de f

   3. $-1 = f(1)$ definição de f

   4. $1 = -1$ transitividade da igualdade aplicada a 2. e 3.

   Determine o erro.

8 Exercícios

1. (a) Apresente uma interpretação que torne a fórmula bem formada $p(x) \wedge \exists y\, q(y) \rightarrow \forall x\, p(x)$ falsa.

   (b) Usando a alínea anterior que pode dizer sobre a afirmação "$p(x) \wedge \exists y\, q(y) \vdash \forall x\, p(x)$"?

2. Traduza logicamente as frases seguintes:

   (a) "Para quaisquer dois números reais x e y existe sempre um número real z tal que $x + z = y$."
   usando $d(x, y, z)$ com o significado de "$x + z = y$"e considerando que $\mathbb{R}$ é o universo.

   (b) "Todos os portugueses falam português mas nem todos falam francês."
   usando $n(x)$, $p(x)$ e $f(x)$ com o significado de, respectivamente, "x é português", "x fala português"e "x fala francês", e considerando como universo todas as pessoas.

3. Prove formalmente que das premissas $\exists x\, M(x)$, $\forall x\, (M(x) \rightarrow \exists y\, C(x, y))$ e $\forall x\, ((\exists y\, C(x, y)) \rightarrow F(x))$ se deduz que $\exists y\, F(y)$. Pode usar as regras de inferência da Tabela RI e as eliminações e introduções universais e existenciais.

4. (a) Diga quando é que uma fórmula bem formada de cálculo de predicados se diz válida.

   (b) Para cada uma das fbf's seguintes, diga, justificando, se é ou não válida:

      i. $\forall x\, (p(x) \rightarrow p(x) \wedge q(x))$
      ii. $\forall x\, (p(x) \rightarrow p(x) \vee q(x))$

5. (a) Verifique se a fórmula bem formada $(\forall z \exists w\, p(z, w)) \rightarrow (\forall z\, p(z, c))$ é ou não uma tautologia (i.e., se é válida).

   (b) Considere a seguinte sequência de fbf's do cálculo de predicados:

1. $\forall z \exists w\, p(z, w)$	premissa
2. $\exists w\, p(z, w)$	1. e EU
3. $p(z, c)$	2. e EE
4. $\forall z\, p(z, c)$	3. e IU

   Tendo em conta a resposta à alínea (a), poderá esta sequência ser uma demonstração formal correcta de que $\forall z \exists w\, p(z, w) \vdash \forall z\, p(z, c)$? Se não, indique as incorrecções.

6. Seja $P(x)$ a afirmação "O estudante x fala japonês"e seja $Q(y)$ a afirmação "O curso y tem um estudante que fala japonês".
   (a) Considerando para universo de discurso o conjunto de todos os estudantes dos cursos de engenharia, traduza as frases seguintes em fórmulas bem formadas de cálculo de predicados.
   (a1) Há pelo menos um estudante que fala japonês.
   (a2) Nenhum estudante fala japonês.
   (b) Considerando para universo de discurso o conjunto de todos os cursos de engenharia, traduza as frases seguintes em fórmulas bem formadas de cálculo de predicados.
   (b1) Todo o curso tem algum estudante que fala japonês.
   (b2) Existe pelo menos um curso onde nenhum estudante fala japonês.

7. Considere as proposições e os predicados seguintes:

c: "Chove."	t: "É Outubro."	b: "É Abril."	$f(x)$: "x fica em casa."
$p(x)$: "x vai à praia."	$g(x,y)$: "x protege y."	m(x,y): "x é mãe de y."	

   Traduza logicamente as frases, considerando para universo do discurso todas as pessoas:
   (i) "Se chove então é Outubro ou Abril."
   (ii) "Se chove a Ana fica em casa."(Pode representar "Ana"por "A".)
   (iii) "Se não chove todos vão à praia."
   (iv) "Toda a mãe protege os seus filhos."

8. (a) Diga quando é que duas fórmulas bem formadas do cálculo de predicados se dizem logicamente equivalentes.
   (b) Apresente uma interpretação para a qual a fórmula bem formada $p(t) \wedge \forall x q(x)$ seja verdadeira e $\forall x(p(x) \wedge q(x))$ seja falsa.
   (c) As duas fórmulas da alínea anterior serão logicamente equivalentes? Justifique.
   (d) Atendendo às alíneas anteriores, é evidente que não se pode deduzir $\forall x(p(x) \wedge q(x))$ de $p(t)$ e $\forall x q(x)$. Descubra então o(s) erro(s) da seguinte demonstração formal:

1. $\forall x q(x)$	premissa
2. $q(t)$	1 e EU
3. $p(t)$	premissa
4. $p(t) \wedge q(t)$	3, 2 e LC
5. $\forall x(p(x) \wedge q(x))$	4 e IU

(e) Faça uma demonstração formal do teorema: $\forall t p(t), \forall x q(x) \vdash \forall x(p(x) \wedge q(x))$.

9. Nas alíneas seguintes consideram-se as fórmulas bem formadas $\forall y\, a(y) \rightarrow \forall y\, b(y)$ e $\forall z(a(z) \rightarrow b(z))$.

   (a) Dê um exemplo de um universo e significados para os predicados $a(x)$ e $b(x)$ que tornem $\forall y\, a(y) \rightarrow \forall y\, b(y)$ verdadeira e $\forall z(a(z) \rightarrow b(z))$ falsa. Justifique sucintamente.

   (b) Diga quando é que duas fórmulas bem formadas se dizem logicamente equivalentes. Conclua se $\forall y\, a(y) \rightarrow \forall y\, b(y)$ e $\forall z(a(z) \rightarrow b(z))$ são ou não logicamente equivalentes.

   (c) Faça uma demonstração formal de que $\forall z(a(z) \rightarrow b(z)), \forall y\, a(y) \vdash \forall y\, b(y)$

   (d) Usando as alíneas anteriores, averigue se é ou não correcta cada uma das afirmações:
   (i) $\forall y\, a(y) \rightarrow \forall y\, b(y) \vdash \forall z(a(z) \rightarrow b(z))$ (ii) $\forall z(a(z) \rightarrow b(z)) \vdash \forall y\, a(y) \rightarrow \forall y\, b(y)$

10. Indique o(s) erro(s) na seguinte "demonstração formal"de que de $\forall x \exists y\, (p(x) \rightarrow q(x,y))$ se deduz $\forall z\, (p(z) \rightarrow q(z,c))$:

1. $\forall x \exists y\, (p(x) \rightarrow q(x,y))$	premissa
2. $\exists y\, (p(z) \rightarrow q(z,y))$	1. e EU
3. $p(z) \rightarrow q(z,c)$	2. e EE
4. $\forall z\, (p(z) \rightarrow q(z,c))$	3. e IU

11. (a) Atribuindo ao predicado $p(x,y)$ a interpretação $x+y=0$, apresente, justificando convenientemente, um universo para o qual a fbf $\forall x \exists y\, p(x,y)$

      i. seja verdadeira;
      ii. seja falsa.

   (b) Diga quando é que uma fórmula bem formada do cálculo de predicados se diz contraditória e averigue se a fórmula bem formada $(\forall z \exists w\, p(z,w)) \rightarrow (\forall z\, p(z,c))$ é ou não contraditória.

   (c) Indique o(s) erro(s) na seguinte "demonstração formal"de que de $\forall z \exists w\, p(z,w)$ se deduz $\forall z\, p(z,c)$:

1. $\forall z \exists w\, p(z,w)$	premissa
2. $\exists w\, p(z,w)$	1. e EU
3. $p(z,c)$	2. e EE
4. $\forall z\, p(z,c)$	3. e IU

Capítulo III

Conjuntos, relações e funções

1 Conjuntos

A prática já tida com conjuntos familiariza com os axiomas seguintes:

Axioma da Extensão: Dois conjuntos são iguais se, e somente se, têm os mesmos elementos.

Axioma da Especificação: A cada conjunto A e a cada condição $S(x)$ corresponde um conjunto B cujos elementos são exatacmente os elementos de A para os quais $S(x)$ acontece. Escreve-se $B = \{x \,|\, x \in A \text{ e } S(x)\}$ ou $B = \{x \in A \,|\, S(x)\}$[1].

É bem conhecida a relação $\subseteq$ entre conjuntos:

$$A \subseteq B \Leftrightarrow \forall x \,(x \in A \Rightarrow x \in B)$$

$$A = B \Leftrightarrow (A \subseteq B \text{ e } B \subseteq A)$$

O *conjunto vazio* designa-se por $\emptyset$ ou $\{\,\}$.
O *conjunto universal* designar-se-á por E, a menos que seja explicitado o contrário.

[1] Também se usa dois pontos, vírgula ou ponto e vírgula em vez de $|$.

Operações entre conjuntos

Operação		Significado	Diagrama de Venn
Intersecção	$\cap$	$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$	
Reunião	$\cup$	$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$	
Complementação	$.^c$	$x \in A^c \Leftrightarrow \neg(x \in A)$	
Diferença	$-$	$x \in A - B \Leftrightarrow x \in A \wedge \neg(x \in B)$	

Lista síntese da relação entre operações lógicas e operações entre conjuntos:

equivalência	identidade
implicação	inclusão
conjunção	intersecção
disjunção	reunião
negação	complementação

Note-se ainda a correspondência existente entre os seguintes conjuntos e condições:

conjunto universal	condição universal
conjunto vazio	condição vazia

Observe o paralelismo existente entre as propriedades sobre operações entre conjuntos enumeradas na tabela seguinte e as propriedades sobre operações lógicas listadas na Tabela CP (na Secção 3 do Capítulo I).

Tabela PC

$A \cup A^c = E$ $A \cap A^c = \emptyset$	Lei da complementação Lei da exclusão
$A \cap E = A$ $A \cup \emptyset = A$	Leis da identidade
$A \cup E = E$ $A \cap \emptyset = \emptyset$	Leis da absorção
$A \cup A = A$ $A \cap A = A$	Leis da idempotência
$(A^c)^c = A$	Lei da dupla complementação
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Leis da comutatividade
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	Leis da associatividade
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Leis da distributividade
$(A \cap B)^c = A^c \cup B^c$ $(A \cup B)^c = A^c \cap B^c$	Leis de De Morgan

Escrevemos $\bigcup\limits_{i \in I} A_i$ para designar a reunião dos conjuntos A_i, $i \in I$, isto é,

$$x \in \bigcup_{i \in I} A_i \text{ se e só se } x \in A_i \text{ para algum } i \in I.$$

Analogamente, $\bigcap\limits_{i \in I} A_i$ denota a intersecção dos conjuntos A_i, $i \in I$.

Se $I = \{1, 2, ..., n\}$, podemos escrever $\bigcup\limits_{i=1}^{n} A_i$ e $\bigcap\limits_{i=1}^{n} A_i$, respectivamente.

Exemplos.

$$\bigcup_{1 \leq i \leq 3} \{1^i,\, 2^i,\, 3^i\} = \{1, 2, 3, 4, 9, 8, 27\} \quad \text{(Verifique.)}$$

$$\bigcap_{1 \leq i \leq 3} \{1^i,\, 2^i,\, 3^i\} = \{1\} \quad \text{(Verifique.)}$$

$$\bigcup_{n \in \mathbb{N} \backslash \{0\}}]-n,\, n[= \mathbb{R} \quad \text{(Verifique.)}$$

$$\bigcap_{n \in \mathbb{N} \backslash \{0\}}]-\frac{1}{n},\, \frac{1}{n}[= \{0\} \quad \text{(Verifique.)}$$

1.1 Exercício: Determine $\bigcap_{n\in\mathbb{N}\setminus\{0\}}]-\frac{1}{n}, \frac{1}{n}[$.

Dois conjuntos A e B dizem-se *disjuntos* se $A \cap B = \emptyset$. Dados conjuntos A_i, $i \in I$, dizemos que eles são *disjuntos dois a dois* se para quaisquer $i, j \in I$, com $i \neq j$, se tem $A_i \cap A_j = \emptyset$.

1.2 Exercício: Em cada uma das seguintes alíneas, diga, justificando, se os conjuntos são ou não disjuntos dois a dois.

(a) $\{2,3,5\}$, $\{4,6,8\}$, $\{11,22\}$

(b) $\{2,3,5\}$, $\{2,4,6\}$, $\{1,7,9\}$

O *cardinal* de um conjunto finito é igual ao número de elementos do conjunto. O cardinal de um conjunto A designa-se por $\#A$, $\mathrm{card}A$ ou $|A|$.

Se A e B são conjuntos finitos, tem-se

$$\mathrm{card}(A \cup B) = \mathrm{card}A + \mathrm{card}B - \mathrm{card}(A \cap B)\,.$$

Para $A_1, ..., A_n$ disjuntos dois a dois, $\mathrm{card}(A_1 \cup ... \cup A_n) = \mathrm{card}A_1 + ... + \mathrm{card}A_n$.

Sejam A e B conjuntos. O *produto cartesiano* de A por B, designa-se por $A \times B$ e é dado por

$$A \times B = \{(a,b) \,:\, a \in A \wedge b \in B\}\,.$$

Analogamente, podemos considerar o produto cartesiano de n conjuntos:

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \,:\, a_1 \in A_1 \wedge a_2 \in A_2 \wedge ... \wedge a_n \in A_n\}\,.$$

Por definição, $A^n = A \times A \times ... \times A$.

Exemplo. Para $A = \{1,2\}$ e $B = \{a,b,c\}$, tem-se que
$A \times B = \{(1,a),\ (1,b),\ (1,c),\ (2,a),\ (2,b),\ (2,c)\}$.

Se A_1, A_2, ..., A_n são conjuntos finitos, então

$$\mathrm{card}(A_1 \times A_2 \times ... \times A_n) = \mathrm{card}A_1 \times \mathrm{card}A_2 \times ... \times \mathrm{card}A_n\,.$$

Seja A um conjunto. O *conjunto potência de A* ou *conjunto das partes de A*, designado por $\mathbb{P}A$ ou 2^A, é o conjunto de todos os subconjuntos de A.

Exemplo. $\mathbb{P}(\{1,2\}) = \{\,\emptyset,\ \{1\},\ \{2\},\ \{1,2\}\,\}$.

Se A é finito, tem-se que

$$\mathrm{card}(\mathbb{P}A) = 2^{\mathrm{card}A}\,.$$

1.3 Exercícios

1. Para $S = \{2, a, 3, 4\}$, $R = \{a, 3, 4, 1\}$, e E o conjunto universal, diga quais das seguintes proposições são verdadeiras.

(a) $a \in S$	(b) $a \in R$	c) $R = S$
(d) $\{a\} \subseteq S$	(e) $\{a\} \in S$	(f) $\emptyset \subseteq R$
(g) $\emptyset \subset R$	(h) $\emptyset \in R$	(i) $\{\emptyset\} \in R$
(j) $E \not\subset R$	(k) $R \subseteq S$	(l) $R \not\subset S$

2. Qual o cardinal dos conjuntos $\emptyset$, $\{a, b\}$, $\{999\}$ e $C = \{1, 2, 3\}$?

3. Determine a reunião, a intersecção e a diferença de A e B, onde $A = \{2^n : n \text{ é inteiro}\}$ e $B = \{\frac{1}{n} : n \text{ é inteiro positivo}\}$

4. Determine $(X \cup Y)^c$, $X^c \cup Y^c$, $X \cup (Y \cap Z)$ e $(X \cup Y) \cap Z$, supondo que:
   (a) o conjunto universal é $E = \{0, 1, 2, ..., 9\}$, $X = \{2, 3, 4\}$, $Y = \{1, 2, 5\}$ e $Z = \{2, 5, 7\}$;
   (b) o conjunto universal é o conjunto N de todos os números inteiros positivos, $X = \{\text{números pares positivos}\}$, $Y = \{\text{números inteiros de 1 a 7}\}$ e $Z = \{2, 5, 7, 8\}$.

5. Mostre que
$$(R \subseteq S) \wedge (S \subset Q) \Rightarrow R \subset Q$$
   É correcto substituir $R \subset Q$ por $R \subseteq Q$? Justifique.

6. (a) Desenhe um diagrama de Venn para dois conjuntos A e B. Determine $A \cap B$ e $A \cap B^c$. A que é igual a reunião de $A \cap B$ com $A \cap B^c$? Verifique que essa igualdade é satisfeita por quaisquer dois conjuntos A e B, usando propriedades das operações de conjuntos.
   (b) Siga um procedimento análogo ao da alínea anterior para concluir que $(A \cup B) \cap (A \cup B^c) = A$.

7. Prove as seguintes igualdades que fazem parte das propriedades das operações sobre conjuntos enumeradas na Tabela PC. O conjunto universal é designado por E.
$$A \cap A = A, \quad A \cap \emptyset = \emptyset, \quad A \cap E = A, \quad A \cup E = E, \quad (A \cap B)^c = A^c \cup B^c$$

8. Prove que a reunião de conjuntos é associativa.

9. Prove que $A \cap A^c = \emptyset$ e $A \cup \emptyset = A$.

10. Partindo das propriedades enumeradas na Tabela PC, prove que, para todo o $n \geq 0$,
    (a) $A \cap (\cup_{i=1}^n B_i) = \cup_{i=1}^n (A \cap B_i)$ (b) $A \cup (\cap_{i=1}^n B_i) = \cap_{i=1}^n (A \cup B_i)$

    (c) $(\cap_{i=1}^n A_i)^c = \cup_{i=1}^n A_i^c$ (d) $(\cup_{i=1}^n A_i)^c = \cap_{i=1}^n A_i^c$

11. Prove que um conjunto A está contido num conjunto B se e só se $A \cap B = A$, se e só se $A \cup B = B$.

12. Simplifique $(A \cup ((B \cup C)^c \cap A^c \cap (B \cap C)^c) \cup A)^c$.

13. (a) Dê exemplos de conjuntos A, B e C tais que $A \cup B = A \cup C$, mas $B \neq C$.
    (b) Prove que $A \cup B = A \cup C$ se e só se $B - A = C - A$.

14. Use propriedades da reunião, da intersecção e da complementação para provar que
$$A \cap (A^c \cup B) = A \cap B.$$

15. Mostre que $(A \cap B) \cup C = A \cap (B \cup C)$ sse $C \subseteq A$.

16. Use diagramas de Venn para mostrar que podemos ter
$$A \cup B \subset A \cup C \text{ mas } B \not\subseteq C$$
$$A \cap B \subset A \cap C \text{ mas } B \not\subseteq C$$
$$A \cap B = A \cap C \text{ mas } B \neq C$$

17. Por meio de diagramas de Venn, e supondo A e B conjuntos tais que $A \cap B \neq \emptyset$, identifique os conjuntos
$$B^c, \quad (A \cup B)^c, \quad B - A^c, \quad A^c \cup B, \quad A^c \cap B.$$

18. Mostre que $(A - B) - C = (A - C) - (B - C)$.

19. Prove que $(A \cap B) \cap (C \cap D) = (A \cap C) \cap (B \cap D)$, usando as relações da Tabela PC.

20. Seja $A = \{1, 2, 3\}$. Determine $A \times (A - \{2\})$ e A^2.

21. Dado $\#A = 4$. Determine $\#(A^3)$ e $\#(2^A)$.

22. Seja $A = \{0, 1, 2\}$. Determine $(A^2 - \{(0, 0)\}) \times A$.

23. Seja $A = \{3, 5, 7\}$ e $B = \{a, b\}$. Determine A^2, B^2, $A \times B$ e $B \times A$.

24. Seja A o conjunto de símbolos do alfabeto português e seja D o conjunto dos algarismos de 0 a 9.

    (a) Determine o número de *strings* de comprimento 3 sobre o alfabeto $A \cup D$.

    (b) Quantos desses *strings* começam com uma letra?

    (c) Quantos *strings* de comprimento 4 ou menor começam com uma letra?

25. Prove que $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

26. Considerando $N = \{1,\ 2,\ ...\}$, o conjunto S de nomes de ruas das cidades de um certo país e C o conjunto das cidades desse país para representar os tipos "cidade", "nome de rua"e "número", represente o tipo "endereço"por meio de um conjunto.

27. Seja A um tipo para todos os clientes e B um tipo para todos os produtos. Existe uma lista de pedidos, contendo o nome do cliente juntamente com o produto pedido. Sabendo que esta lista é para ser tratada como um conjunto, indique o tipo desta lista.

28. Seja $A = \{1, 2, 3\}$ e $B = \{2, 3, 4\}$. Determine o conjunto potência $2^{A \cup B}$.

2 Relações

Sejam A_1, A_2, ..., A_n conjuntos e $A_1 \times A_2 \times ... \times A_n$ o seu produto cartesiano. Uma relação R sobre $A_1 \times A_2 \times ... \times A_n$ consiste num conjunto de n-uplos $(a_1,\ a_2,\ ...,\ a_n)$ com $a_i \in A_i$, $i = 1, 2, ..., n$, ou seja, é dada por um subconjunto de $A_1 \times A_2 \times ... \times A_n$. Como R é uma relação constituída por n-uplos, R diz-se uma relação n-ária.

Exemplo. Uma empresa vende determinados produtos que vamos designar por x, y, z e w. Os clientes são considerados do tipo a, b ou c de acordo com a quantidade de material comprada pelo cliente no último ano civil. Relativamente a um certo dia a empresa registou as vendas de acordo com a tabela seguinte

Cliente	Tipo	Produto	Preço
J. Costa	a	x	50
A. Santos	c	y	15
C. Cardoso	b	y	15
H. Barros	a	w	30

Considerando $C = \{\text{clientes}\}$, $T = \{a, b, c\}$, $P = \{\text{produtos}\}$ e $D = \{\text{preços dos produtos}\}$, associada a esta tabela temos uma relação quaternária constituída pelos seguintes elementos de $C \times T \times P \times D$:

(J. Costa, a, x, 50)
(A. Santos, c, y, 15)
(C. Cardoso, b, y, 15)
(H. Barros, a, w, 30)

2.1 Exercício. Um certo agregado familiar é constituído pelo Paulo, o Rui, o António, o Bernardo, a Marta, a Júlia, a Sara e a Inês, que, para simplificar, vamos designar por p, r, a, b, m, j, s e i, respectivamente. As suas relações familiares são as seguintes: Do António e da Júlia nasceram a Marta e a Sara. Da Marta e do Bernardo nasceram o Rui e a Inês. Da Sara e do Paulo nasceu a Júlia.

(a) Faça uma árvore descrevendo estas relações.

(b) Seja G o conjunto das pessoas deste agregado familiar. Escreva todos os ternos da relação $R = \{(x, y, z) \in G^3 \, : \, x \text{ é mãe de } y \text{ e } y \text{ é mãe de } z\}$.

No que se segue trataremos de um tipo especial de relações, as relações binárias (a que chamaremos simplesmente relações).

Sejam A e B dois conjuntos. Uma *relação* R de A para B é constituída por um conjunto de pares (x, y) com $x \in A$ e $y \in B$. Se $(x, y) \in R$, dizemos que x é R-relacionado com y. Para exprimir que R é uma relação de A para B, escrevemos $R : A \leftrightarrow B$. A A chamamos *conjunto de partida* de R e a B chamamos *conjunto de chegada* de R.

Uma relação $R : A \leftrightarrow B$ pode ser vista como um subconjunto de $A \times B$. Assim, $A \times B$ é ele próprio uma relação, a *relação universal* de A para B. Por sua vez a *relação vazia* não contém nenhum par.

Exemplo. Seja P o conjunto das províncias de Portugal e C o conjunto das cidades portuguesas. Seja R a relação de P para C tal que, dados $x \in P$ e $y \in C$, x está R-relacionado com y se e só se a província x contém a cidade y. Deste modo, os pares (Beira

Alta, Viseu) e (Algarve, Faro) pertencem à relação R, enquanto que o par (Minho, Viseu) lhe não pertence.

Existem várias maneiras de expressar relações. Como uma relação $R : A \leftrightarrow B$ é um subconjunto de $A \times B$, podemos expressar relações usando a notação dos conjuntos. Dada uma relação R também é habitual escrever

$$xRy$$

para significar $(x, y) \in R$. Por vezes usamos

$$x \not R y$$

com o significado de $\neg(xRy)$.

As relações finitas podem ser representadas por matrizes booleanas, isto é, matrizes cujas entradas são constituídas por 0's e 1's. Com efeito, sejam $A = \{a_1, a_2, ..., a_m\}$ e $B = \{b_1, b_2, ..., b_n\}$ e consideremos A e B ordenados segundo a ordem natural dos índices dos seus elementos. A matriz $m \times n$

$$M_R = (a_{ij}^R)$$

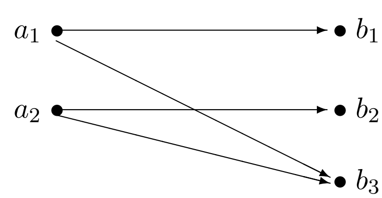
de uma relação $R : A \leftrightarrow B$ é definida por

$$a_{ij}^R = \begin{cases} 0 \text{ se } a_i \not R b_j \\ 1 \text{ se } a_i R b_j \end{cases} .$$

Exemplo. Sejam $A = \{2, 3, 4, 5\}$ e $B = \{1, 2, 3\}$. Consideremos os elementos de A e B ordenados pela ordem natural. Seja R a relação "é múltiplo de". A matriz desta relação é

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

As relações podem também ser representadas graficamente. Uma forma de representar uma relação $R : A \leftrightarrow B$ é colocar os elementos de A à esquerda, os de B à direita e, por cada $(x, y) \in R$, ligar x a y por meio de um arco dirigido. Por exemplo,



representa a relação $\{(a_1, b_1), (a_1, b_3), (a_2, b_2), (a_2, b_3)\}$ de $\{a_1, a_2\}$ para $\{b_1, b_2, b_3\}$.

Seja $R : A \leftrightarrow B$ uma relação. O *domínio* de R, abreviadamente, dom$R$, é dado por

$$\text{dom}R = \{x \in A \, : \, \exists_{y \in B}(x, y) \in R\} \, .$$

O *contradomínio* de R, abreviadamente, cdom$R$, é o seguinte subconjunto de B

$$\text{cdom}R = \{y \in B \, : \, \exists_{x \in A}(x, y) \in R\} \, .$$

Se A é um conjunto e R é uma relação de A para A, dizemos que R é uma *relação em* A ou *sobre* A. A relação $I_A = \{(x, x) \, : \, x \in A\}$ diz-se a *relação identidade* sobre A.

Novas relações a partir de relações dadas:

Se $R : X \leftrightarrow Y$ é uma relação, então a *relação inversa* $R^{-1} : Y \leftrightarrow X$ é constituída por todos os pares (y, x) tais que $(x, y) \in R$. Assim, $yR^{-1}x$ sse xRy. É claro que

$$(R^{-1})^{-1} = R \, .$$

Todas as operações feitas com conjuntos podem ser feitas com relações. Assim, dadas duas relações R e S com os mesmos conjuntos de partida e os mesmos conjuntos de chegada, tem-se:

$$x(R \cap S)y \Leftrightarrow xRy \wedge xSy$$

$$x(R \cup S)y \Leftrightarrow xRy \vee xSy$$

$$x(R - S)y \Leftrightarrow xRy \wedge x\not{S}y$$

$$x(R^c)y \Leftrightarrow x\not{R}y$$

Se $R : A \leftrightarrow B$ e $S : C \leftrightarrow D$ são duas relações tais que $A \subseteq C$, $B \subseteq D$ e $R \subseteq S$, dizemos que

S é uma *extensão* de R
e R é uma *restrição* de S.

Sejam $R : X \leftrightarrow Y$ e $S : Y \leftrightarrow Z$ duas relações. A *composição de* R *e* S, denotada por $R \cdot S$, tem X como conjunto de partida, Z como conjunto de chegada e é constituída por todos os pares (x, z) para os quais existe algum objecto $y \in Y$ tal que $(x, y) \in R$ e $(y, z) \in S$. Ou seja,

$$x(R \cdot S)z \Leftrightarrow \exists_{y \in Y}(xRy \wedge ySz) \, .$$

A composição de relações é associativa.

Seja R uma relação sobre um conjunto A. Geralmente abreviamos $R \cdot R$ por R^2, $R \cdot R \cdot R$ por R^3, etc.

Matrizes booleanas e representação de relações:

Nas matrizes booleanas o 1 corresponde a **V** (verdadeiro) e 0 corresponde a **F** (falso).

A *soma booleana* de duas matrizes booleanas $A = (a_{ij})$ e $B = (b_{ij})$ da mesma ordem, é dada por

$$A \bigvee B = (a_{ij} \vee b_{ij}) \, .$$

O *produto booleano* de uma matriz booleana $A = (a_{ij})$ $m \times n$ por uma matriz booleana $B = (b_{ij})$ $n \times p$ é dado por

$$A \odot B = \left(\bigvee_{k=1}^{n} a_{ik} \wedge b_{kj} \right) \, .$$

Como já vimos, a matriz de uma relação é booleana. Se duas relações $R : X \leftrightarrow Y$ e $S : Y \leftrightarrow Z$ são representadas pelas matrizes M_R e M_S, respectivamente, então a matriz da relação $R \cdot S$ é

$$M_{R \cdot S} = M_R \odot M_S \, .$$

2.2 Exercícios

1. Sejam $R, S : A \leftrightarrow B$ relações de matrizes M_R e M_S, respectivamente. Determine as matrizes de $R \cup S$, $R \cap S$, R^c e R^{-1} em função de M_R e M_S.

2. Sejam $P = \{(1,2),(2,4),(3,3)\}$ e $Q = \{(1,3),(2,4),(4,2)\}$. Determine $P \cup Q$, $P \cap Q$, $\mathrm{dom}(P)$, $\mathrm{dom}(P \cup Q)$, $\mathrm{cdom}(P)$, $\mathrm{cdom}(Q)$ e $\mathrm{cdom}(P \cap Q)$.

3. Mostre que se P e Q são duas relações sobre um mesmo conjunto,

$$\mathrm{dom}(P \cup Q) = \mathrm{dom}(P) \cup \mathrm{dom}(Q)$$

e

$$\mathrm{cdom}(P \cap Q) \subseteq \mathrm{cdom}(P) \cap \mathrm{cdom}(Q).$$

4. Quais são os contradomínios das relações

$$S = \{(x, x^2) \,|\, x \in \mathbb{N}\} \quad \text{e} \quad T = \{(x, 2x) \,|\, x \in \mathbb{N}\}$$

onde $\mathbb{N} = \{0, 1, 2, ...\}$?

5. Seja M a relação "menor ou igual do que"e D a relação "divide". Ambas M e D estão definidas no conjunto $\{1, 2, 3, 6\}$. Escreva M e D sob a forma de conjuntos e determine $M \cap D$.

6. Um grupo de pessoas está sentado à volta de uma mesa. Sabendo que xRy significa que x está sentado à direita de y, expresse a relação B em função de R sabendo que xBy significa que x está ou à direita ou à esquerda de y.

7. Sejam $R : X \leftrightarrow X$ e $S : U \leftrightarrow V$. Determine os conjuntos de partida de $R \cap S$, $R \cup S$ e R^c.

8. Seja xPy verdadeiro se x é pai ou mãe de y e seja xSy verdadeiro se x é irmã de y. Expresse a "relação tia"como composição destas duas relações.

9. Suponha que S é a relação $\subset$ como definida habitualmente para conjuntos. Determine S^c e S^{-1}.

10. Seja $R = \{(1, a), (2, b), (1, c)\}$ e $S = \{(a, A), (a, B), (c, D)\}$. Determine $R \cdot S$.

11. Seja $R = \{(1, 2), (1, 3), (3, 4)\}$. Determine R^2 e R^3.

12. Seja xRy verdadeiro sse $x = y - 1$. Determine xR^2y e $x(R \cup R^2)y$.

13. Seja $R = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$ sobre $\{1, 2, 3, 4\}$. Determine M_R e M_{R^2}.

3 Propriedades das relações. Relações de equivalência

Seja R uma relação sobre um conjunto X. R diz-se:

reflexiva, se, para todo o $x \in X$, xRx;

irreflexiva, se, para todo o $x \in X$, $x \not R x$;

simétrica, se, para cada x e y em X, $xRy \Rightarrow yRx$;

anti-simétrica, se, para cada x e y em X com $x \neq y$, $xRy \Rightarrow y \not R x$; ou seja, se xRy e yRx então $x = y$;

transitiva, se, para cada x, y e z em X, $xRy \wedge yRz \Rightarrow xRz$.

3.1 Exercício. Caracterize a matriz de uma relação (sobre um conjunto finito)
(i) reflexiva; (ii) irreflexiva; (iii) simétrica; (iv) anti-simétrica.

Fechos

Seja R uma relação sobre um conjunto A.

De entre todas as relações reflexivas em A que contêm R existe uma que está contida nas outras todas, ou seja, é a menor relação reflexiva que contém R. O *fecho reflexivo* de R denota-se por $R^{(r)}$ e é precisamente a menor relação reflexiva em A que contém R. Analogamente se definem *fecho simétrico* e *fecho transitivo*, isto é, o primeiro é a menor relação simétrica que contém R e o segundo é a menor relação transitiva que contém R. Denotam-se por $R^{(s)}$ e R^+, respectivamente.

Por R^* denotamos a menor relação reflexiva e transitiva contendo R.

Facilmente se concluem as seguintes igualdades:

$$R^{(r)} = R \cup I_A$$

$$R^{(s)} = R \cup R^{-1}$$

$$R^+ = R \cup R^2 \cup R^3 \cup ... \cup R^m, \text{supondo que } R \text{ é sobre um conjunto } A \text{ tal que } |A| = m.$$

$$R^* = R^+ \cup R^0, \text{denotando por } R^0 \text{ a relação identidade sobre } A.$$

3.2 Exercício Prove que se R é uma relação sobre um qualquer conjunto, finito ou infinito, então $R^+ = \bigcup_{k=1}^{\infty} R^k$.

Relações de equivalência

Uma relação R sobre um conjunto diz-se uma *relação de equivalência* se for reflexiva, simétrica e transitiva.

Uma *partição* dum conjunto S é uma família $(A_i)_{i \in I}$ de subconjuntos de S, tal que cada elemento de S está em exactamente um dos conjuntos A_i; ou seja, para cada $s \in S$, existe um e só um $i \in I$ tal que $s \in A_i$.

Teorema. *Seja R uma relação de equivalência em S, e seja $[x]$ o conjunto de todos os $y \in S$ R-relacionados com x, i.e., $[x] = \{y : yRx\}$. Então os subconjuntos $[x]$ de S determinam uma partição de S.*

Reciprocamente, toda a partição de um conjunto S determina uma relação de equivalência.

Aos conjuntos $[x] = \{y : yRx\}$ determinados por uma relação de equivalência R chamamos *classes de equivalência* da relação R.

Exemplo. Seja R a relação no conjunto dos números inteiros tal que aRb se e só se $|a| = |b|$. Verifica-se facilmente que se trata de uma relação reflexiva, simétrica e transitiva, sendo portanto uma relação de equivalência. As classes de equivalência correspondentes são dadas por $[a] = \{-a, a\}$, para cada inteiro a.

Seja n um inteiro positivo. Dois números inteiros a e b dizem-se *congruentes módulo* n, escrevendo-se $a \equiv b \pmod{n}$, quando $a - b$ é múltiplo de n. Verifique que a relação de congruência é uma relação de equivalência. Quais são as classes de equivalência?

3.3 Exercícios

1. Indique todas as propriedades das seguintes relações sobre o conjunto $\{1, 2, 3\}$. Quais delas são relações de equivalência?

   (a) $R_1 = \{(1, 2), (2, 2)\}$

   (b) $R_2 = \{(1, 2), (2, 3), (1, 3), (2, 1)\}$

   (c) $R_3 = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$

   (d) $R_4 = \{(1, 2), (2, 3)\}$

2. Indique todas as propriedades da relação identidade, da relação vazia e da relação universal.

3. Dê um exemplo de uma relação que seja ao mesmo tempo simétrica e anti-simétrica.

4. Mostre que, se S e R são relações reflexivas, então $R \cup S$ e $R \cap S$ também são reflexivas.

5. Se as relações R e S são reflexivas, simétricas e transitivas mostre que $R \cap S$ é também reflexiva, simétrica e transitiva.

6. Seja $R = \{(1,2),(4,3),(2,2),(2,1),(3,1)\}$ uma relação sobre $S = \{1,2,3,4\}$. Determine o fecho simétrico, o fecho reflexivo e o fecho transitivo de R.

7. Dado $S = \{1,2,3,...,10\}$ e a relação $R = \{(x,y) \mid x+y = 10\}$ sobre S, quais as propriedades de R?

8. (a) Quais são as entradas da matriz de $R \cap R^{-1}$ que poderão ser não nulas se R for uma relação anti-simétrica?

   (b) Se R for uma relação reflexiva e anti-simétrica sobre um conjunto de cardinalidade n, qual é a matriz de $R \cap R^{-1}$?

9. Determine as matrizes das relações R^{-1}, R^2, R^3 e $R \cdot R^{-1}$, sabendo que R é uma relação no conjunto $\{a,b,c\}$ cuja matriz é

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

10. Prove que S^{-1} é uma relação de equivalência se e só se S é uma relação de equivalência.

11. Sejam R e S duas relações de equivalência representadas pelas matrizes

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

respectivamente. Mostre que $R \cdot S$ não é uma relação de equivalência.

12. (a) Mostre que dois números inteiros a e b são congruentes módulo n se e só se o resto da divisão de a por n é igual ao resto da divisão de b por n.

    (b) Mostre que a relação de congruência módulo n entre números inteiros é uma relação de equivalência.

    (c) Descreva as classes de equivalência dessa relação de equivalência.

13. Prove que se R e S são duas relações de equivalência que têm as mesmas classes de equivalência, então a sua composição é uma relação de equivalência.

14. Para cada uma das seguintes relações, indique as suas propriedades. Diga se a relação é reflexiva, irreflexiva, simétrica, anti-simétrica ou transitiva. Determine também se a relação é uma relação de equivalência. Todas as relações são no conjunto de todos os humanos.

    (a) xRy representa que x é filho de y.

    (b) xRy representa que x é descendente de y.

    (c) xRy representa que x é o marido de y.

    (d) xRy representa que x é a cônjugue de y.

    (e) xRy representa que x e y têm os mesmos pais (pai e mãe).

    (f) xRy representa que x é tão alto ou mais baixo do que y.

15. O que podemos concluir sobre uma relação cuja matriz é triangular superior?

16. Para cada uma das relações seguintes, indique se é reflexiva (r), irreflexiva (i), simétrica (s), anti-simétrica (a), ou transitiva (t).

    (a) Sejam x e y números inteiros e xRy verdadeira se x divide y.

    (b) Sejam x e y pessoas e xRy verdadeira se x e y pertencem ao mesmo agregado familiar.

    (c) Sejam x e y rapazes e xRy verdadeira se x e y são irmãos ou $x = y$.

    (d) Sejam x e y pessoas e xRy verdadeira se x e y são primos.

17. Indique, justificando, quais das relações dadas no exercício anterior são de equivalência.

18. Seja $R = \{(a, b), (b, d), (c, b), (d, a)\}$. Determine a matriz da relação. Determine ainda

    (i) a matriz do fecho reflexivo,

    (ii) a matriz do fecho simétrico,

    (iii) a matriz do fecho transitivo.

4 Ordens parciais

Uma relação R sobre um conjunto S diz-se uma *ordem parcial (fraca)* se for reflexiva, anti-simétrica e transitiva; R diz-se uma *ordem parcial estrita* se for irreflexiva, anti-simétrica e transitiva.

Um conjunto A com uma ordem parcial R diz-se um *conjunto parcialmente ordenado* (ou *poset*). Denotamo-lo por (A, R) ou simplesmente por A se não houver ambiguidade sobre a ordem R que estamos a considerar.

Se R for uma ordem parcial estrita, o seu fecho reflexivo é uma ordem parcial fraca. Por exemplo, a relação $<$ entre números inteiros é uma relação de ordem estrita (Justifique). O seu fecho reflexivo é precisamente a relação $\leq$.

Por outro lado, se R for uma ordem parcial em A, então $R - I_A$ é uma ordem parcial estrita.

Uma ordem parcial R sobre A diz-se uma *ordem total* ou *ordem linear* se, para todos os x, y em A se tem sempre que xRy ou yRx. Neste caso, o poset (A, R) diz-se *conjunto totalmente ordenado* ou *cadeia*.

Exemplos de cadeias são os números naturais, os números inteiros e os números reais, cada um destes conjuntos considerado com a relação $\leq$.

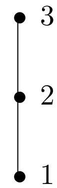
Seja $\preceq$ uma ordem parcial em A. Denotamos por $\prec$ a correspondente ordem parcial estrita, i.e., a ordem parcial estrita obtida de $\preceq$ tirando-lhe todos os pares (x, x) com $x \in A$.

A inversa de $\prec$ denota-se por $\succ$ e a inversa de $\preceq$ denota-se por $\succeq$. Se $(A, \preceq)$ é um conjunto parcialmente ordenado, $(A, \succeq)$ também é um conjunto parcialmente ordenado e diz-se o *dual de* $(A, \preceq)$.

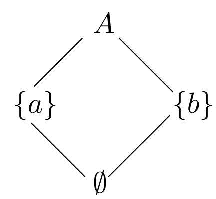
Seja $(A, \preceq)$ um conjunto parcialmente ordenado. Se $x \prec y$, dizemos que x é um *predecessor* de y, ou que y é um *sucessor* de x. Se $x \prec y$ e não existem elementos entre x e y, i.e., não existe nenhum $z \in A$ tal que $x \prec z \prec y$, dizemos que x é um *predecessor imediato* de y, ou que y é um *sucessor imediato* de x.

Um conjunto parcialmente ordenado pode ser representado por um *diagrama de Hasse*: representamos os elementos do conjunto e sempre que x é um predecessor imediato de y ligamos x a y por um arco com x situado num nível inferior a y.

Claro que o diagrama de Hasse de uma cadeia é muito simples. Por exemplo, o diagrama de Hasse do conjunto $\{1, 2, 3\}$ com a relação $\leq$ habitual é



Para $A = \{a, b\}$, o diagrama de Hasse do poset $(\mathbb{P}A, \subseteq)$ é



Conjuntos parcialmente ordenados bem-fundados

Seja $(A, \preceq)$ um conjunto parcialmente ordenado. Uma sequência (finita ou infinita) $< x_1, x_2, ... >$ em A diz-se uma *sequência estritamente decrescente* relativamente à ordem $\preceq$ se satisfizer $x_i \succ x_{i+1}$ para todo i.

Um poset $(A, \preceq)$ diz-se *bem-fundado* se não tiver sequências estritamente decrescentes infinitas.

Exemplos.

1. No poset $(\mathbb{Z}, \leq)$, a sequência $< 2, 1, -2, -10 >$ é estritamente decrescente.

   É claro que $(\mathbb{Z}, \leq)$ tem sequências estritamente decrescentes infinitas (dê um exemplo), pelo que não é bem-fundado.

   Por outro lado, $(\mathbb{N}, \leq)$ é bem-fundado (justifique).

2. Relativamente a $(\mathbb{P}A, \subseteq)$, com $A = \{a, b, c\}$, um exemplo de sequência estritamente decrescente é $< A, \{a, b\}, \{b\}, \{\,\} >$. Trata-se obviamente de um poset bem-fundado, já que o respectivo conjunto é finito.

   Mas se $\mathbb{P}A$ for infinito, isso já não acontece. Por exemplo, a sequência

   $$< \mathbb{N} - \{0, 1\}, \mathbb{N} - \{0, 1, 2\}, ... >$$

   onde o i-ésimo termo é $\mathbb{N} - \{0, 1, ..., i\}$, é uma sequência estritamente decrescente infinita e, portanto, $(\mathbb{P}\mathbb{N}, \subseteq)$ não é bem-fundado.

Ordens parciais em produtos cartesianos

Sejam $(A_1, \leq_1)$ e $(A_2, \leq_2)$ dois conjuntos parcialmente ordenados. Indicamos a seguir dois tipos de ordem parcial que podemos obter para $A_1 \times A_2$ a partir de $\leq_1$ e $\leq_2$:

1. $(x_1, x_2) \preceq (y_1, y_2)$ sse $x_i \leq_i y_i$ para $i = 1, 2$.
2. A chamada *ordem lexicográfica* é dada por: $(x_1, x_2) \preceq_l (y_1, y_2)$ sse $x_1 <_1 y_1$ ou $x_1 = y_1$ e $x_2 \leq_2 y_2$, onde $<_1$ designa a relação de ordem parcial estrita correspondente a $\leq_1$.

Analogamente podemos definir ordens parciais para produtos cartesianos de 3, 4, ... conjuntos.

Por exemplo, se $(A_i, \leq_i)$ são conjuntos parcialmente ordenados para $i = 1, 2, 3$, então a respectiva ordem lexicográfica em $A_1 \times A_2 \times A_3$ é dada por:
$(x_1, x_2, x_3) \preceq_l (y_1, y_2, y_3)$ sse $(x_1 <_1 y_1) \vee (x_1 = y_1 \wedge x_2 <_2 y_2) \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 \leq_3 y_3)$.

4.1 Exercícios

1. Averigue se as relações dadas nas alíneas dos exercícios 1, 14 e 16 de 3.3 são relações de ordem fraca ou estrita.
2. Considere a relação XRY sse $X \subseteq Y$, no conjunto $\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.
   (a) Mostre que R é uma relação de ordem parcial
   (b) Faça o seu diagrama de Hasse.
3. Considere a relação $x \sqsubseteq y$ sse "x divide y"no conjunto $\{2, 3, 5, 6, 9, 10, 12\}$.
   (a) Mostre que é uma relação de ordem parcial.
   (b) Será total?
   (c) Faça o seu diagrama de Hasse.
4. O conjunto $\mathbb{N}$ é bem-fundado relativamente à relação $\leq$. E relativamente à relação $\geq$?
5. Considere o conjunto parcialmente ordenado constituído por $\mathbb{Z}$ com a relação $\leq$. Trata-se de um conjunto bem-fundado? E se em vez de $\leq$ considerarmos $\geq$?
6. (a) Dados conjuntos parcialmente ordenados $(A_1, \leq_1)$ e $(A_2, \leq_2)$, mostre que a relação definida no conjunto $A_1 \times A_2$ por $(x_1, x_2) \preceq (y_1, y_2)$ sse $x_i \leq_i y_i$ para $i = 1, 2$.é efectivamente uma ordem parcial.

(b) Mostre que se $(A_i, \leq_i)$ são conjuntos totalmente ordenados para $i = 1, 2, 3$ então $A_1 \times A_2 \times A_3$ com a respectiva ordem lexicográfica é também um conjunto totalmente ordenado.

Generalize este resultado a n conjuntos A_i.

5 Funções

Uma relação binária $f \subseteq A \times B$ diz-se uma *função* se para cada $x \in A$ existir um e um só $y \in B$ tal que $(x, y) \in f$. Uma relação $(n+1)$-ária $g \subseteq A_1 \times A_2 \times ... \times A_n \times B$ diz-se uma função se para cada $(x_1, x_2, ..., x_n) \in A_1 \times A_2 \times ... \times A_n$, existir um e um só $y \in B$ tal que $(x_1, x_2, ..., x_n, y_n) \in g$.

Notações. Usualmente para significar que $(x, y) \in f$, escrevemos $f(x) = y$ ou $f : x \mapsto y$. Se f é uma função de A para B, escrevemos $f : A \to B$.

De notar que o *domínio* e o *contradomínio* de uma função f no sentido já conhecido coincidem com o domínio e contradomínio de $f$considerada como uma relação. Portanto, dada uma função $f : A \to B$, $\mathrm{dom} f = A$ e $\mathrm{cdom} f = \{y \in B \mid \exists x \in A (y = f(x))\}$.

Algumas funções importantes

1. *Função identidade*: A função identidade num conjunto A é a função $I_A : A \to A$ definida por $f(x) = x$ para todo o $x \in A$, coincidindo portanto com a relação identidade.

2. *Função constante*: é uma função tal que todos os elementos do domínio têm a mesma imagem.

3. *Função característica*: A *característica* de um número real x é o maior número inteiro que é menor ou igual a x e denota-se por $[x]$. Assim, por exemplo, $[-\frac{3}{2}] = -2$, $[-0.24] = -1$ e $[2.5] = 2$. A função característica faz corresponder a cada número real x a sua característica $[x]$.

4. *Função módulo n*: Dados um número inteiro x e um inteiro positivo n, existem um inteiro y e um natural r com $0 \leq r < n$, tais que $x = yn + r$, sendo y e r únicos. Como é bem sabido, y é o quociente da divisão de x por n e r é o resto dessa divisão. Facilmente se conclui que $y = [\frac{x}{n}]$. O resto da divisão de x por n diz-se x módulo n e representa-se por $x \,\mathrm{mod}\, n$. Por exemplo, 8 mod3=2 e -8 mod3=1. A função módulo n faz corresponder a cada número inteiro x, o número $x \,\mathrm{mod}\, n$. A igualdade seguinte relaciona a função módulo n com a função característica:

$$x \,\mathrm{mod}\, n = x - [x/n]\, n\,.$$

Recorde que uma função $f : A \to B$ diz-se:

- *injectiva*, se quaisquer dois elementos distintos do domínio têm imagens diferentes, i.e., $\forall_{x,\, x' \in A}\, (f(x) = f(x') \to x = x')$;
- *sobrejectiva*, se todo o elemento do conjunto de chegada é imagem de algum elemento do domínio, expresso doutro modo, se $\forall_{y \in B}\, \exists_{x \in A}\, (f(x) = y)$;
- *bijectiva*, se for injectiva e sobrejectiva, ou seja, $\forall_{y \in B}\, \exists^1_{x \in A}\, (f(x) = y)$.

Funções parciais

Uma relação binária $f \subseteq A \times B$ diz-se uma *função parcial* se para cada $x \in A$ existir quando muito um $y \in B$ tal que $(x, y) \in f$.

Por exemplo, a relação $\{(2, a), (3, a), (4, b)\}$ é uma função parcial de $\{1, 2, 3, 4\}$ para $\{a, b\}$.

Claro que uma função é, em particular, uma função parcial. De uma função parcial podemos obter uma função restringindo o conjunto de partida ao domínio da função parcial.

Composição de funções

A composição de funções define-se como a das relações. Se tivermos duas funções $f : A \to B$ e $g : B \to C$, a relação composição de f com g é sempre uma função. Mas atenção: a notação usada para as funções é diferente da usada para as relações; nomeadamente, se usarmos $\cdot$ como símbolo da composição entre funções e utilizarmos $\cdot_r$ como símbolo da composição entre relações, temos $g \cdot f = f \cdot_r g$. Portanto, para cada $x \in A$,

$$(g \cdot f)(x) = g(f(x))\,.$$

Tal como a composição de relações, a composição de funções é associativa.

Podemos considerar uma composição de funções mais geral do que a descrita acima: basta que o contradomínio de f seja um subconjunto do domínio de g, ou seja, basta que $g(f(x))$ esteja definido para todo o x do domínio de f.

É também possível fazer a composição de funções parciais. Dadas uma função parcial f de A em B e uma função parcial g de B em C, a composição $g \cdot f$ das duas é a função parcial de A em C tal que $\mathrm{dom}(g \cdot f) = \{x \in A \,|\, x \in \mathrm{dom} f \text{ e } f(x) \in \mathrm{dom} g\}$ e que a cada x do seu domínio faz corresponder $g(f(x))$.

Por exemplo, sejam f e g as funções parciais definidas de $\mathbb{R}$ para $\mathbb{R}$ por $f(x) = x + 1$ e $g(y) = 1/y$. Então a sua composição faz corresponder a cada $x \neq -1$ o número $g(f(x)) = \frac{1}{x+1}$.

Visto que uma função é uma relação, podemos falar da sua relação inversa. Assim, por exemplo, a relação $\{(1,2),(2,3),(3,3)\}$ é uma função de $X = \{1,2,3\}$ em X e a sua relação inversa é $\{(2,1),(3,2),(3,3)\}$. Mas esta relação não é uma função: a 3 correspondem duas "imagens".

Dizemos que uma função f tem inversa, ou é *invertível*, se a sua relação inversa for uma função, que se diz então a *função inversa de* f.

É evidente que uma função não injectiva não tem inversa. (Porquê?)

Uma função que não seja sobrejectiva também não tem inversa. (Porquê?)

Portanto, podemos concluir que uma função para ter inversa tem de ser bijectiva. A recíproca também é verdadeira. Na verdade, se $f : A \to B$ é uma função bijectiva, $f^{-1} : A \to B$ define-se fazendo corresponder a cada $y \in B$ o único x de A tal que $f(x) = y$.

Se uma função $f : A \to B$ é bijectiva, a sua inversa, $f^{-1} : B \to A$, também o é. (Porquê?) Além disso, $f \cdot f^{-1} = I_B$ e $f^{-1} \cdot f = I_A$.

Se uma função $f : A \to B$ é injectiva mas não sobrejectiva, podemos considerar uma inversa parcial. Por exemplo, a função $f : [-\pi/2,\, \pi/2] \to \mathbb{R}$ tal que $f(x) = \sin x$, para cada x, é injectiva mas não é sobrejectiva; no entanto, restringindo o conjunto de chegada de f a $[-1,\, 1]$, obtemos a inversa $g : [-1,\, 1] \to [-\pi/2,\, \pi/2]$ que a cada $x \in [-1,\, 1]$ faz corresponder $\arcsin x$.

Cardinal de um conjunto

É bem sabido que um conjunto finito tem cardinal n se e só se existir uma bijecção entre esse conjunto e o conjunto $\{1, 2, ..., n\}$. É também claro que dois conjuntos finitos têm o mesmo cardinal sse existir uma função bijectiva entre eles. Vamos estender a noção de cardinal a conjuntos finitos.

Dois conjuntos A e B dizem-se *equipotentes* se existir uma função bijectiva de A para B. Note-se que a relação $\sim$ entre conjuntos dada por

$$A \sim B \Leftrightarrow (\text{existe uma função bijectiva de } A \text{ para } B)$$

é uma relação de equivalência. Portanto, dois conjuntos são equipotentes se pertencerem à mesma classe de equivalência dessa relação.

Dizemos que dois conjuntos A e B têm o mesmo *cardinal* sse forem equipotentes. Escreve-se então card$A$ =card$B$.

Exemplos.

1. car($\mathbb{N}$)=card($\{n \in \mathbb{N} : n \text{ é par}\}$); uma função que o permite concluir é a que faz corresponder a cada número natural o seu dobro. (Verifique.)

Analogamente, o cardinal do conjunto dos naturais ímpares é igual ao de $\mathbb{N}$ e igual ao cardinal do conjunto dos naturais múltiplos de 3. (Indique funções que justifiquem estas afirmações. Determine outros subconjuntos de $\mathbb{N}$ que têm o mesmo cardinal que $\mathbb{N}$.)

2. Para mostrar que card$(\mathbb{Z}^+ \times \mathbb{Z}^+) =$card$\mathbb{N}$, podemos usar a *diagonalização de Cantor* (veja nos apontamentos da aula). Verifique que a diagonalização de Cantor define uma função bijectiva $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{N}$ tal que

$$f((i,j) = \sum_{k=1}^{i+j-1} (k-1) \; + i\,,$$

ou seja,

$$f(i,j) = \frac{(i+j-2)(i+j-1)}{2} \; + i\,.$$

3. card$\mathbb{Q}$ =card$\mathbb{N}$

4. card$\mathbb{R}$ >card$\mathbb{N}$.

Um conjunto infinito A diz-se *numerável* se card$A$ =card$\mathbb{N}$.

Portanto, exemplos de conjuntos numeráveis são $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, etc. O conjunto $\mathbb{R}$ é um exemplo de conjunto não numerável.

5.1 Exercícios

1. Quais das seguintes relações são funções e quais são funções parciais de $X = \{1,2,3\}$ para $Y = \{1,2,3,4\}$? Em cada caso, indique o domínio e o contradomínio da relação.

   $f_1 = \{(1,3),(2,3),(3,3)\}$

   $f_2 = \{(1,3),(1,4),(2,3),(2,4)\}$

   $f_3 = \{(1,1),(2,2),(3,3)\}$

   $f_4 = \{(1,2)\}$

2. Verifique se os conjuntos seguintes definem funções (considerando um conveniente conjunto de partida). Em caso afirmativo, indique o domínio e o contradomínio.

   (a) $\{(1,(2,3)),(2,(3,4)),(3,(1,4)),(4,(2,4))\}$

   (b) $\{(1,(2,3)),(2,(3,4)),(1,(2,4))\}$

   (c) $\{((1,2),3),((2,3),4),((3,3),2)\}$

   (d) $\{(1,(2,3)),(2,(2,3)),(3,(2,3))\}$

3. Mostre que, fazendo corresponder a cada A de $\mathbb{P}(D)$, onde D é um conjunto, o seu complementar A^c, obtemos uma função.

4. Será a relação "é subconjunto de"entre os subconjuntos de um dado conjunto uma função?

5. Considere as funções f, g e h dadas por $f = \{(1, c), (2, a), (3, b), (4, c)\}$, $g = \{(a, 2), (b, 1), (c, 4)\}$ e $h = \{(1, A), (2, B), (3, D), (4, D)\}$. Determine $g \cdot f$, $h \cdot (g \cdot f)$, $h \cdot g$ e $(h \cdot g) \cdot f$. Determine também $f \cdot g$.

6. Sejam as funções de variável real $f(x) = 3x^2 + y$, $g(x) = \frac{x}{y}$ e $h(x) = (x + y)^2$. Determine $f \cdot g$, $g \cdot f$, $f \cdot h$ e $f \cdot g \cdot h$.

7. Determine quais das seguintes funções são injectivas, quais são sobrejectivas e quais são bijectivas.

   (a) $f : \{1, 2, 3\} \longrightarrow \{a, b, c\} \qquad f = \{(1, a), (2, b), (3, c)\}$

   (b) $g : \{1, 2, 3\} \longrightarrow \{a, b, c, d\} \qquad g = \{(1, a), (2, b), (3, c)\}$

   (c) $h : \{1, 2, 3\} \longrightarrow \{1, 2, 3\} \qquad h = \{(1, 2), (2, 1), (3, 2)\}$

   (d) $p : \mathbb{N} \longrightarrow \mathbb{N} \qquad p(j) = j^2 + 2$

   (e) $m : \mathbb{N} \longrightarrow \mathbb{N} \qquad m(j) = j(\text{mod}3)$

   (f) $q : \mathbb{N} \longrightarrow \mathbb{N} \qquad q(j) = \begin{cases} 1 & \text{se } j \text{ é ímpar} \\ 0 & \text{se } j \text{ é par} \end{cases}$

   (g) $r : \mathbb{N} \longrightarrow \{0, 1\} \qquad r(j) = \begin{cases} 0 & \text{se } j \text{ é ímpar} \\ 1 & \text{se } j \text{ é par} \end{cases}$

8. Sendo $(0...p) = \{0, 1, 2, ..., p\}$, quais das seguintes funções são injectivas, sobrejectivas ou bijectivas?

   (a) $f : \mathbb{Z} \longrightarrow \mathbb{Z} \qquad f(j) = \begin{cases} j/2 & \text{se } j \text{ par} \\ (j-1)/2 & \text{se } j \text{ ímpar} \end{cases}$

   (b) $f : (0...6) \longrightarrow (0...6) \qquad f(x) = (3x)(\text{mod}7)$

   (c) $f : (0...3) \longrightarrow (0...3) \qquad f(x) = (3x)(\text{mod}4)$

9. Demonstre que se f e g são funções injectivas então $f \cdot g$, supondo que está definida, também é injectiva.

10. Indique todas as funções possíveis de $X = \{a, b\}$ para $Y = \{0, 1\}$ e diga quais são injectivas, sobrejectivas ou bijectivas.

11. Se X e Y são conjuntos finitos, determine uma condição necessária para a existência de uma função injectiva de X para Y.

12. Prove que se A é um conjunto finito toda a função de A para A que é injectiva também é sobrejectiva e vice-versa. Mostre que o mesmo não acontece para conjuntos infinitos.

13. Mostre que as funções f e g, ambas de $\mathbb{N} \times \mathbb{N}$ para $\mathbb{N}$ dadas por $f(x, y) = x + y$ e $g(x, y) = xy$ são sobrejectivas mas não injectivas.

14. Seja $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^3 - 2$. Determine f^{-1}.

15. Indique uma função injectiva de $A \times B$ para $B \times A$, sendo A e B conjuntos quaisquer. Essa função é sobrejectiva?

16. Seja $X = \{1, 2, 3, 4\}$. Defina uma função $f : X \to X$ tal que $f \neq I_X$ e f injectiva. Determine f^2, f^3, f^{-1} e $f \cdot f^{-1}$.

17. Determine uma função injectiva $g : X \to X$ tal que $g \neq I_X$ mas $g \cdot g = I_X$.

18. Determine $[5/2]$, $[(5/2)^2]$, $[5/2]^2$, $4 - [5/2]$ e $4 + [-5/2]$.

19. Para $n = 1, 2, ..., 10$, indique o valor de $n \text{mod} 3$ e $(-n) \text{mod} 3$.

20. Seja $y = x(x+1)$, $x \in \mathbb{N}$. Defina $h(y)$ como sendo z se $z(z+1) \leq y < (z+1)(z+2)$. Expresse $h(y)$ usando a função característica. Defina a função resto associada com este $h(y)$.

21. Prove que:
    (a) $x^2 - [x]^2 < 2[x] + 1$, para todo o real $x \geq 0$;
    (b) $x^2 - [x]^2 > 2[x] + 1$, para todo o real $x < 0$.

22. Dado $D = \{1, 2, 3\}$
    (a) Enumere D^3 usando a ordem lexicográfica.
    (b) Enumere D^2 usando a diagonalização de Cantor.

23. Prove que o conjunto dos números racionais é numerável.

6 Exercícios

1. Tomando $\{-3,-2,-1,0,1,2,3,4\}$ para conjunto universal, $A = \{-2, 2\}$, $B = \{1, 2, 3, 4\}$ e $C = \{x \mid x \geq 0 \wedge x^2 < 9\}$,

   (a) determine o cardinal de C;

   (b) determine (em extensão) os conjuntos $A \cap C$, $A - B$, B^c, $A \cup B^c$, $B \times C$ e 2^A.

2. Em cada uma das alíneas seguintes diga se a igualdade apresentada é ou não válida para todos os conjuntos A e B. No caso afirmativo deduza a igualdade e no caso negativo exiba um contra-exemplo.

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

3. Em cada um dos três casos, (A), (B) e (C), descreve-se uma relação R definida num certo conjunto:

   (A) xRy sse $x \bmod 2 = y \bmod 2$, no conjunto $\mathbb{Z}$ dos números inteiros;
   (B) XRY sse $X \subseteq Y$, no conjunto das partes de $\{0,\ 1\}$;
   (C) XRY sse $X \cap Y \neq \emptyset$, no conjunto $\{\emptyset, \{1\},\ \{2\},\ \{1,2\}\,\}$.

   (a) Faça corresponder a cada um dos casos (A), (B) e (C), a situação que, de entre (i), (ii) e (iii), a seguir, lhe diz respeito, justificando sucintamente:

      (i) R é uma relação de ordem parcial;
      (ii) R é uma relação de equivalência;
      (iii) R não é relação de ordem parcial nem relação de equivalência.

   (b) Para o caso em que R é uma relação de equivalência, indique as respectivas classes de equivalência.

   (c) Para o caso em que a relação não é relação de ordem parcial nem relação de equivalência, escreva (em extensão) o conjunto dos pares de R, e indique o seu fecho reflexivo.

4. (a) Diga quando é que uma relação é uma função e quando é função parcial.

   (b) para cada uma das relações S seguintes, definidas de $\mathbb{Z}$ para $\mathbb{Z}$, diga se é função, apenas função parcial ou nem uma coisa nem outra. Justifique sucintamente no caso de não ser função.

   i. $(x, y) \in S$ sse $x + y > 0$; ii. $(x, y) \in S$ sse $y = x^2$; iii. $(x, y) \in S$ sse $y = \dfrac{1}{x}$

5. Averigue se a seguinte igualdade entre conjuntos é verdadeira ou falsa, provando-a ou apresentando um contra-exemplo.

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

6. Dado o conjunto $A = \{a, \{a\}\}$, determine

   (a) $A \cap \{a\}$;

   (b) o conjunto $A - \{\{a\}\}$;

   (c) o conjunto potência de A;

   (d) o conjunto $A \times A$.

7. Considere as relações R e S definidas no conjunto dos números inteiros tais que xRy significa que $x \leq y$ e xSy significa que $x = 2y$.

   (a) Diga, justificando convenientemente, se S é reflexiva, irreflexiva, simétrica, anti-simétrica ou transitiva.

   (b) Indique o significado de $xR \cdot Sy$. Averigue se $(1001, 2222)$ pertence a $R \cdot S$.

   (c) Considere agora as relações R e S definidas no conjunto $A = \{1, 2, 4\}$. Determine sob a forma de subconjunto de $A \times A$:

   (i) R (ii) S (iii) $R \cdot S$ (iv) $R \cdot S^{-1}$

8. (a) Quando é que uma relação é uma função?

   (b) O estudante A tenta definir uma função $g : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ usando a regra $g(\frac{m}{n}) = (m, n)$ para todos os inteiros m e n com $n \neq 0$. O estudante B afirma que g está mal definida, ou seja, g não é função. Mostre que quem tem razão é o estudante B.

9. Dados o conjunto $A = \{\, \emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\}\, \}$ (onde $\emptyset$ designa o conjunto vazio),

   (a) indique os cardinais de A, A^3 e 2^A;

   (b) determine

   (i) $A - \{\{\emptyset\}\}$, (ii) $\{x,\ y\} \times (A - \{\{\emptyset\}\})$, (iii) $A \cap \emptyset$, (iv) $A \cap \{\{\emptyset\}\}$.

10. (a) Mostre que para quaisquer conjuntos A, B e C, se $A \cup B = A \cup C$ então $B - A = C - A$.

    (b) Arranje conjuntos A, B e C tais que $A \cup B = A \cup C$ mas $B \neq C$.

11. Considere no universo dos humanos as relações F, B e N definidas por

    xFy sse x é filho(a) de y

    xBy sse x é irmã(o) de y

    xNy sse x é neto(a) de y

    (a) Determine qual é a relação de parentesco dada por $F \cdot B$.

    (b) Expresse a relação N em função de F.

12. A relação R definida no conjunto $V = \{a, e, i, o, u\}$ é, relativamente à ordenação alfabética dos seus elementos, representada pela matriz

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

    (a) Escreva R sob a forma de conjunto de pares ordenados.

    (b) Diga, justificando, se R é uma relação de ordem parcial (fraca) e, em caso afirmativo, desenhe o seu diagrama de Hasse.

    (c) Determine a matriz da relação $R \cdot R$.

13. (a) Quando é que uma relação é uma função?

    (b) Quando é que uma função se diz injectiva?

    (c) Averigue se a função $f : \{-1, 0, 1, 2\} \to \mathbb{N}$ definida por $f(x) = (2x) \bmod 6$ é ou não injectiva.

Capítulo IV

Indução e Recursão

1 Os números naturais, Axiomas de Peano

Os números naturais são bem conhecidos. Vamos considerar o 0 como fazendo parte dos números naturais. Portanto os números naturais são

$$0, 1, 2, 3, ...$$

Dizemos que 3 é o *sucessor* de 2, 2 é o sucessor de 1, 1 é o sucessor de 0. O número natural 0 é o único que não é sucessor de nenhum. Podemos obter todos os números naturais considerando 0, o sucessor de 0, $s(0) = 1$, o sucessor do sucessor de 0, $s(s(0)) = 2$, e por aí fora. Os *Axiomas de Peano*, enumerados a seguir, apresentam os números naturais. A partir deles podemos deduzir propriedades já bem conhecidas.

Axiomas de Peano:

1. 0 é um número natural.
2. Se n é um número natural, também $s(n)$ é um número natural.
3. Para todo n, $s(n) > 0$.
4. Se $s(n) = s(m)$, então $m = n$.
5. $\forall m(m + 0 = m)$
6. $\forall m \forall n(m + s(n) = s(m + n))$
7. $\forall n(n \times 0 = 0)$
8. $\forall m \forall n(m \times s(n) = m \times n + m)$
9. Dada uma propriedade P relativa aos números naturais, é válido o Princípio de Indução Matemática $P(0) \wedge \forall n(P(n) \rightarrow P(s(n))) \rightarrow \forall n P(n)$

1.1 Exercícios.

1. Seja $n = s(s(2))$. Determine $s(s(s(n)))$.

2. Defina $x \leq y$ para todos os números naturais usando apenas o mecanismo do sucessor.

3. Em vez dos números naturais 0, 1, 2, ..., considere as sequências seguintes:

   (a) 0, 1, 2, 0, 1, 2, ...

   (b) 3, 4, 5, ...

   (c) 0, 1, 2, 3, 3, 3, 3, ...

   Para cada uma das sequências, indique quais dos primeiros quatro axiomas de Peano se verificam. Suponha que $s(n)$ designa o elemento imediatamente a seguir na sequência.

4. (*) Construa um modelo que não satisfaça o terceiro axioma de Peano mas satisfaça $\forall m(m + 0 = m)$ e $\forall m \forall n(m + s(n) = s(m + n))$.

2 Indução Matemática

O último axioma de Peano, o Princípio de Indução Matemática, diz-nos que:
Se uma dada propriedade
(i) é satisfeita por 0; e
(ii) para todo o $n \geq 0$, sempre que é satisfeita por n também o é por $n + 1$;
então todo o número natural satisfaz a propriedade.

Escrevendo $P(n)$ com o significado de "n satisfaz a propriedade P", este princípio pode ser esquematizado do seguinte modo:

$$\begin{array}{l} P(0) \\ \forall n(P(n) \rightarrow P(n+1) \\ \hline \\ \therefore \forall P(n) \end{array}$$

Dizemos que a propriedade se verifica para a *base indutiva* se tivermos $P(0)$. Quando, para cada n, provamos que $P(n) \Rightarrow P(n + 1)$, dizemos que se trata do *passo indutivo.* Assim, no passo indutivo, para cada n, provamos $P(n + 1)$ a partir da hipótese $P(n)$. Dá-se então a $P(n)$ o nome de *hipótese indutiva.*

2.1 Exemplo. Vamos usar indução matemática para provar que $n^3 + 2n$ é divisível por 3, para todo o $n \in \mathbb{N}$.

A propriedade $P(n)$ é, neste caso, "$n^3 + 2n$ é divisível por 3".

$P(0)$ significa que $0^3 + 2 \times 0$ é divisível por 3, o que é obviamente verdadeiro.

Assumindo agora como hipótese que $P(n)$ se verifica, vamos provar $P(n+1)$. Temos que

$$\begin{aligned}(n+1)^3 + 2(n+1) &= (n+1)[(n+1)^2 + 2] \\ &= (n+1)(n^2 + 2n + 1 + 2) \\ &= n^3 + 2n^2 + 3n + n^2 + 2n + 3 \\ &= (n^3 + 2n) + 3n^2 + 3n + 3\end{aligned}$$

Por hipótese indutiva, $n^3 + 2n$ é divisível por 3; por outro lado, é claro que $3n^2 + 3n + 3$ é divisível por 3. Logo $(n+1)^3 + 2(n+1)$ é divisível por 3, completando-se assim o passo indutivo.

Nos Exemplos de 2.2 a 2.3 são provadas algumas das propriedades da adição e da multiplicação de números naturais usando o Princípio de Indução Matemática, bem como outros dos axiomas de Peano.

Sugestão. Os Exemplos 2.2, 2.3 e 2.4 usam indução matemática para demonstrar algumas das propriedades conhecidas sobre números naturais a partir dos axiomas de Peano. Se ainda não se sente bem familiarizado com a indução matemática, será melhor praticar primeiro esta técnica nos Exemplos 2.1 e 2.5, e nos exercícios no final das Secções 2, 3 e 11, antes de uma leitura cuidada dos Exemplos 2.2, 2.3 e 2.4.

2.2 Exemplo. Usando os axiomas de Peano, vamos provar a propriedade comutativa da adição de números naturais, i.e.,

$$\forall m \forall n (m + n = n + m)\,.$$

<u>Demonstração por indução sobre m</u>:

<u>Base indutiva</u>: $P(0)$, i.e., $\forall n(0 + n = n + 0)$. Provamos $P(0)$ por <u>indução sobre n</u>:

Base indutiva: 0+0=0+0

Hipótese indutiva: $0 + n = n + 0$

Passo indutivo:

1. $0 + s(n) = s(0 + n)$, por axioma 6.
2. $s(n) + 0 = s(n) = s(n + 0)$, por axioma 5.
3. $s(0 + n) = s(n + 0)$, por hipótese indutiva
4. $0 + s(n) = s(n) + 0$, por 1,2 e 3 e transitividade da igualdade

Conclusão: $\forall n(0 + n = n + 0)$

Hipótese indutiva: $P(m)$, ou seja, $\forall n(m+n=n+m)$

Passo indutivo: Queremos provar que $\forall n(s(m)+n=n+s(m))$. Fixemos n; vamos mostrar que $s(m)+n=n+s(m)$.

$n+s(m)=s(n+m)$, pelo axioma 6.
$\quad\quad = s(m+n)$, pela hipótese indutiva.

Vamos provar por indução sobre n que, para todo o natural n, se verifica $s(m+n)=s(m)+n$:

Base indutiva: A igualdade $s(m+0)=s(m)+0$ é verdadeira porque $s(m+0)=s(m)=s(m)+0$, pelo axioma 5.

Hipótese indutiva: $s(m+n)=s(m)+n$

Passo indutivo: Prova-se que $s(m+s(n))=s(m)+s(n)$.

$s(m+s(n))=s(s(m+n))$, pelo axioma 5.
$\quad\quad = s(s(m)+n)$, pela hipótese indutiva
$\quad\quad = s(m)+s(n)$, pelo axioma 5.

Conclusão: $\forall n(s(m+n)=s(m)+n)$

Conclusão: $\forall m\forall n(m+n=n+m)$

2.3 Exercício. Usando os axiomas de Peano, prove a propriedade associativa da adição, i.e., $\forall m\forall n\forall r((m+n)+r=m+(n+r))$.

2.4 Exemplo. Vamos provar a propriedade distributiva da multiplicação em relação à adição para números naturais, i.e., $\forall m\forall n\forall r(m\times(n+r)=m\times n+m\times r)$.

Fixados m e n, prova-se que $\forall r(m\times(n+r)=m\times n+m\times r)$:

Demonstração por indução sobre r:

Base indutiva: $m\times(n+0)=m\times n=m\times n+0=m\times n+m\times 0$, usando os axiomas 5. e 7.

Hipótese indutiva: $P(r)$, ou seja, $m\times(n+r)=m\times n+m\times r$.

Passo indutivo: Queremos provar que $m\times(n+s(r))=m\times n+m\times s(r)$

$m\times(n+s(r))=m\times s(n+r)$, pelo axioma 6,
$\quad\quad = m\times(n+r)+m$, pelo axioma 8,
$\quad\quad = (m\times n+m\times r)+m$, pela hipótese indutiva,
$\quad\quad = m\times n+(m\times r+m)$, pela assoc. da adição,
$\quad\quad = m\times n+m\times s(r)$, pelo axioma 8.

Conclusão: $\forall r(m\times(n+r)=m\times n+m\times r)$.

A Indução Matemática pode ser usada partindo de uma base diferente de 0. Isto é, em vez de provarmos que $P(n)$ se verifica para todo o $n \geq 0$ podemos provar que $P(n)$ se verifica para todo o $n \geq n_0$. O quadro seguinte esquematiza o Princípio de Indução Matemática com a base indutiva $n_0 \neq 0$.

$P(n_0)$ $\forall n((n \geq n_0) \to (P(n) \to P(n+1)))$ ――――――――――― $\therefore \forall n((n \geq n_0) \to P(n))$	Base indutiva: $P(n_0)$ Hipótese indutiva: $P(n)$, com $n \geq n_0$ Passo indutivo: $P(n) \Rightarrow P(n+1))$ Conclusão: verifica-se $P(n)$ para todo o $n \geq n_0$

2.5 Exemplo. Vamos provar que $2^n < n!$ para $n \geq 4$.

(i) A propriedade verifica-se para $n = 4$: $2^4 = 16 < 4! = 4 \times 3 \times 2 = 24$.

(ii) Seja agora n um número natural maior ou igual a 4 tal que $2^n < n!$. Queremos mostrar que $2^{n+1} < (n+1)!$. Temos:

$$\begin{aligned} 2^{n+1} &= 2^n \times 2 \\ &< n! \times 2, \text{ pela hipótese indutiva} \\ &< n! \times (n+1), \text{ visto que } 4 \leq n, \text{ logo } 2 < 5 < n+1 \\ &= (n+1)! \end{aligned}$$

Logo $2^{n+1} < (n+1)!$.

Concluimos por (i) e (ii) que para todo o $n \geq 4$ se verifica a desigualdade $2n < n!$.

Observação: Note que a propriedade se não verifica para $n = 1, 2, 3$.

O <u>Princípio de Indução Matemática Forte</u> usa uma hipótese indutiva mais forte. O quadro seguinte esquematiza este princípio.

$P(0)$ $\forall n((\forall k((mk \leq n) \to P(k))) \to P(s(n)))$ ――――――――――― $\therefore \forall n P(n))$	Base indutiva: $P(0)$ Hipótese indutiva: $P(k)$ para todo $k \leq n$ Passo indutivo: Assumindo a hipótese indutiva, prova-se $P(n+1))$ Conclusão: verifica-se $P(n)$ para todo o n

Portanto, neste caso, no passo indutivo, temos de provar que, para cada natural $n \geq 0$

se a propriedade se verifica para todos os naturais menores ou iguais a n também se verifica para $n+1$.

2.6 Exemplo. Vamos provar que todo o número natural maior do que 1 pode ser escrito como produto de números primos.

(i) A propriedade é válida para $n = 2$, visto que 2 é um produto de primos com um único factor, o próprio 2.

(ii) Suponhamos agora a propriedade válida para todo o natural k tal que $2 \leq k \leq n$. Pretendemos mostrar que $n+1$ se pode escrever como um produto de primos. Temos duas possibilidades: ou $n+1$ é primo sendo nesse caso trivialmente um produto de primos, ou $n+1$ não é primo, ou seja, existem dois números naturais a e b maiores do que 1 tais que

$$n+1 = a \times b.$$

Mas então temos que

$$2 \leq a, b < n+1$$

Pela hipótese indutiva, a escreve-se como um produto de primos e b também se escreve como um produto de primos. Logo o produto de a por b é um prouto de primos, como queríamos provar.

De (i) e (ii), conclui-se o pretendido.

2.7 Exercícios.

1. Prove que $2+4+6+\cdots+2n = n(n+1)$ para todo o $n \geq 1$.

2. Prove que $3^n \leq (2n)!$ para $n \geq 2$.

3. Prove que $2^n \geq n^2$ para $n \geq 4$.

4. Mostre que 7 divide $2^{3n} - 1$ para todo $n \in \mathbb{N}$.

5. Mostre que 5 divide $n^5 - n$ para todo $n \in \mathbb{N}$.

6. Use indução matemática para mostrar que se $h > 0$ então $1 + nh \leq (1+h)^n$ para todo o inteiro não negativo n.

7. Mostre que com moedas de 2 e 5 euros se pode perfazer um total de n euros para qualquer $n \geq 4$.

8. Uma estação de correio vende selos de 9 e 10 cêntimos. Demonstre que qualquer tarifa de 79 cêntimos ou superior pode ser paga com uma combinação destes selos.

9. Mostre que no cálculo proposicional toda a expressão lógica que não contém negações tem um número ímpar de símbolos.

10. Use indução matemática para provar que um conjunto não vazio com n elementos tem $n(n-1)/2$ subconjuntos contendo exactamente dois elementos.

11. Os números harmónicos H_k, $k = 1, 2, 3, ...$, definem-se por

$$H_k = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{k}\,.$$

   (a) Determine o valor de H_3 e de H_{2^2}.

   (b) Use indução matemática para mostrar que, para todo o $n \in \mathbb{N}$,

$$H_{2^n} \geq 1 + \frac{n}{2}\,.$$

12. Use indução matemática para mostrar que $\neg(p_1 \vee p_2 \vee ... \vee p_n)$ é equivalente a $\neg p_1 \wedge \neg p_2 \wedge ... \wedge \neg p_n$, onde p_1, p_2, ..., p_n são proposições.

13. Mostre que

$$[(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge ... \wedge (p_{n-1} \to p_n)] \to [(p_1 \wedge p_2 \wedge .... \wedge p_{n-1}) \to p_n]\,.$$

14. Descubra o erro na seguinte "prova"de que todos os cavalos são da mesma cor.

   Seja $P(n)$ a afirmação de que todos os cavalos de um conjunto com n cavalos têm a mesma cor. É claro que $P(1)$ se verifica. Suponhamos agora que $P(n)$ é verdadeiro, ou seja, que todos os cavalos de um conjunto de n cavalos são da mesma cor. Consideremos $n + 1$ cavalos; numeremos esses cavalos por 1,2, 3, ..., n, $n + 1$. Por hipótese indutiva, os primeiros n desses cavalos são da mesma cor, e do mesmo modo os últimos n cavalos também são da mesma cor. Como o conjunto dos n primeiros cavalos e o conjunto dos últimos n cavalos se intersectam, concluimos então que os $n+1$ cavalos são todos da mesma cor. Fica assim provado que $P(n + 1)$ é verdadeiro, o que finaliza a prova por indução.

15. Descubra o erro na seguinte "prova"de que $a^n = 1$ para todo o $n \in \mathbb{N}$.

   Base indutiva: $a^0 = 1$ é verdadeiro por definição de a^0.

   Hipótese indutiva: $a^k = 1$ para todo o $k \in \mathbb{N}$ tal que $k \leq n$.

   Passo indutivo:

$$a^{n+1} = a^{2n-(n-1)} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1\,.$$

16. (*) A partir dos axiomas de Peano, demonstre que a adição é associativa. Pode usar as propriedades da adição já provadas nesta secção.

17. (*) A partir dos axiomas de Peano, demonstre que 0 é um zero à esquerda para a multiplicação. Por outras palavras, prove que $0 \times n = 0$.

3 Definições recursivas

Comecemos por um exemplo de definição recursiva, neste caso, a definição de "descendente de x":

1. Todos os filhos de x são descendentes de x.

2. Filhos de descendentes de x são descendentes de x.

Uma <u>definição recursiva</u> consiste numa <u>regra de base</u> e numa <u>regra recursiva</u>.
A regra de base descreve os elementos definidos directamente.
Os outros elementos são definidos por aplicação sucessiva da regra de recursão a partir do(s) elemento(s) definido(s) pela regra base.

3.1 Exemplo. <u>Definição recursiva de operadores</u>.

Se $\otimes$ é um operador com identidade e, $\displaystyle\bigotimes_{i=m}^{n} a_i$ define-se recursivamente por

1. $\displaystyle\bigotimes_{i=m}^{n} a_i = e$, se $m > n$;

2. $\displaystyle\bigotimes_{i=m}^{n+1} a_i = \bigotimes_{i=m}^{n} a_i \otimes a_{n+1}$, se $m \leq n+1$.

3.2 Exercício. Prove a seguinte propriedade dos somatórios: $\displaystyle\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n} a_i + \sum_{i=m}^{n} b_i$.

3.3 Exemplos. A seguir apresentam-se mais dois exemplos de definições recursivas.

I. Uma SL-expressão (i.e., uma "simplified logical expression") é definida recursivamente do seguinte modo:

1. Todas as variáveis proposicionais são SL-expressões.

2. Se A e B são duas SL-expressões, também $(A \wedge B)$, $(A \vee B)$ e $\neg A$ são SL-expressões.

II. Uma SM-expressão é definida recursivamente por:

1. Todos os inteiros e variáveis nominais são SM-expressões.
2. Se A e B são duas SM-expressões, também $-A$, $(A + B)$, $(A - B)$ e $(A \times B)$ são SM-expressões.

3.4 Exercícios.

1. Mostre que $1^2 + 2^2 + ... + n^2 = n(n+1)(2n+1)/6$ para todo o inteiro positivo.
2. Determine uma fórmula para
$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + ... + \frac{1}{n(n+1)}$$
analisando os valores da expressão para os primeiros valores de n. Use indução matemática para provar que a conclusão a que chegou está correcta.
3. (a) Prove por indução que para todo o natural n se verifica
$$\sum_{k=1}^{n}(2k-1) = n^2.$$
   (b) Use o resultado da alínea anterior para calcular a soma de todos os números inteiros ímpares de 1 a 99, ou seja, $1 + 3 + 5 + 7 + ... + 95 + 97 + 99$.
4. Indique todos os termos de $\sum_{i=1}^{3}(\sum_{j=0}^{2} a_{ij})$.
5. Simplifique $\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} a_{i+1}$.
6. Prove as seguintes propriedades dos somatórios, usando indução matemática (supõe-se $m \geq 1$)):

(S1) $\displaystyle\sum_{i=m}^{n}(a_i+b_i)=\sum_{i=m}^{n}a_i+\sum_{i=m}^{n}b_i$

(S2) $\displaystyle\sum_{i=m}^{n}(a_i+b)=(\sum_{i=m}^{n}a_i)+(n-m+1)b,\ n\geq m-1$

(S3) $\displaystyle\sum_{i=m}^{n}(a_ib)=b\sum_{i=m}^{n}a_i$

(S4) $\displaystyle\sum_{i=1}^{n}a_i=\sum_{i=1+k}^{n+k}a_{i-k}$

7. Use indução matemática para provar que:

   (a) $\neg\bigwedge_{i=1}^{n}P_i=\bigvee_{i=1}^{n}\neg P_i$;

   (b) $(\prod_{i=1}^{n}a_i)^2=\prod_{i=1}^{n}a_i^2$.

8. Prove que $\sum_{i=0}^{n}i(i+1)=n(n+1)(n+2)/3$, se $n\geq 0$.

9. Prove por indução sobre m a seguinte igualdade:

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}=\sum_{j=1}^{n}\sum_{i=1}^{m}a_{ij}$$

10. Prove que para todo $n\in\mathbb{N}$ se verifica a igualdade

$$\sum_{i=0}^{n}i\cdot i!=(n+1)!-1\,.$$

11. Prove que para todo $n\in\mathbb{N}$ se verifica a igualdade

$$\sum_{j=0}^{n}j^4=n(n+1)(2n+1)(3n^2+3n-1)/30\,.$$

12. Mostre que, para todo o natural $n\geq 1$,

$$\sum_{\emptyset\neq\{a_1,\dots,a_k\}\subseteq\{1,2,\dots,n\}}\frac{1}{a_1a_2\dots a_k}=n\,.$$

13. Considere a definição recursiva de SM-expressão dada no final desta secção antes dos exercícios. Descreva como é que aplicando um número finito de vezes as regras 1 e 2 pode obter a SM-expressão $(((x-2)+(2\times 3))-y)$.

14. Considere todas as fbfs do cálculo proposicional onde figuram apenas os conectivos lógicos $\neg$ e $\rightarrow$. Dê uma definição recursiva dessas fórmulas.

15. Um certo conjunto A de números define-se recursivamente do seguinte modo:

    1. $1 \in A$;
    2. Se $n \in A$ então também $n+3 \in A$.

       (Nenhuns outros números pertencem a A.)

       Identifique A, justificando.

16. Dê uma definição recursiva do conjunto de todas as potências de 2 com expoente natural.

4 Árvores binárias

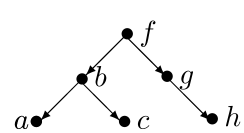
Uma *árvore binária* sobre um conjunto C pode definir-se recursivamente do seguinte modo:

1. A árvore vazia é uma árvore binária. Esta árvore denota-se por ( ).

2. Se A e B são duas árvores binárias e $c \in C$, então (A, c, B) é uma árvore binária. A diz-se a subárvore à esquerda e B a subárvore à direita.

A árvore que consiste apenas num vértice c, que segundo a definição recursiva acima se denota por $((), c, ())$, designa-se habitualmenter apenas por (c).

Uma árvore binária pode ser representada graficamente. Por exemplo, a árvore binária $(((a), b, (c)), f, ((\,), g, (h)))$ representa-se do seguinte modo:



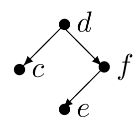
Os elementos a, b, c, ..., dizem-se *vértices* da árvore. Os vértices estão ligados por *arcos*.

Se T é uma árvore e i e j são vértices de T tais que existe um arco dirigido de i para j, diz-se que i é *pai* de j e que j é *filho* de i. Vértices sem filhos dizem-se *folhas*, os vértices com filhos dizem-se *vértices com ramo*. Uma *raiz* é um vértice que não tem pai.

No exemplo acima, b é pai de a e c, f é raiz da árvore, g é um vértice com ramo e h é uma folha.

Árvores binárias não vazias têm uma raiz e cada vértice tem no máximo dois filhos.

4.1 Exercício. Use a definição recursiva de uma árvore binária para descrever a árvore binária representada por



Solução: $((c), d, ((e), f, ()))$

4.2 Exemplo. Suponhamos que pretendemos definir recursivamente todas as árvores binárias não vazias sobre $\{a, b, c\}$ tais que cada vértice tem ou 2 filhos ou 0 filhos.

Comece por representar algumas destas árvores.

Designemos por $\mathcal{A}$ o conjunto das árvores binárias referidas. Verifique que ele pode ser definido por

1. As árvores (a), (b) e (c) pertencem a $\mathcal{A}$.
2. Se A e B são duas árvores binárias e $x \in \mathcal{A}$, então (A, x, B) é uma árvore binária.

4.3 Exercícios.

1. (a) Represente graficamente as árvores binárias $A = ((b), a, ((a), b, (a)))$ e $B = (((a), b, (a)), b, ((b), b, (b)))$.

   (b) Seja $\mathcal{T}$ o conjunto das árvores binárias sobre o conjunto $\{0, 1\}$ definidas recursivamente por:
   1. (0) e (1) pertencem a $\mathcal{T}$.
   2. Se A é uma árvore em $\mathcal{T}$ de raiz 0 e B é uma árvore em $\mathcal{T}$ de raiz 1, então $(A, 0, B)$ e $(B, 1, A)$ pertencem a $\mathcal{T}$.

   Represente todas as árvores de $\mathcal{T}$ de altura menor ou igual a 3.

2. Seja $A = \{0, 1\}$ e seja G o conjunto de todas as árvores binárias T sobre A com a seguinte propriedade: As subárvores à esquerda e à direita de cada nó de T são idênticas na estrutura e nos nós. Dê uma definição recursiva do conjunto G.

5 Listas

Uma *lista* é uma sequência finita de zero ou mais elementos.

Uma *lista* sobre um conjunto A define-se recursivamente por:

1. A lista vazia é uma lista. Esta lista denota-se por [ ].

2. Se $a \in A$ e B é uma lista sobre A, então $[a|B]$ é uma lista. Neste caso, a diz-se a *cabeça* da lista e B é a *cauda* da lista.

Para armazenar os três números 15, 3 e 22, põem-se em lista

$$[15\,|\,[3\,|\,[22]\,]\,]$$

Aqui a cabeça da lista é 15 e $[3\,|\,[22]]$ é a cauda. Esta lista pode ser representada por [15, 3, 22]

Uma lista da forma $[a|[]]$ denota-se por $[a]$.

<u>Outras notações</u>: Para denotar uma lista da forma $[a\,|\,[\,b\,|\,[c]\,]\,]$ também se usa $[a, [b, [c]]]$ ou $< a, < b, < c >>>$ ou $< a, b, c >$.

5.1 Exemplo. Pretende-se definir o conjunto S de todas as listas não vazias sobre o conjunto $\{0, 1\}$ onde os elementos em cada lista alternam entre 0 e 1.

Temos então que $S = \{[0], [1], [1, 0], [0, 1], [0, 1, 0], [1, 0, 1], ...\}$.

Neste caso, S pode definir-se recursivamente por:

Base: [0], [1] pertencem a S.

Recursão: Se B pertence a S então: $[1, B]$ pertence a S, se a cabeça de B é 0 e $[0, B]$ pertence a S se cabeça de B é 1.

5.2 Exercícios.

1. (a) Seja $\mathcal{L}$ o conjunto de listas sobre o conjunto $\{0, 1, t\}$ definido recursivamente a seguir, onde $c(L)$ denota a cabeça da lista L:

   1. $[\,] \in \mathcal{L}$;
   2. Dada $L \in \mathcal{L}$:

      (i) se L tem cabeça e $c(L) = t$, então $[0,\ L]$ e $[1,\ L]$ pertencem a $\mathcal{L}$;

      (ii) caso contrário, então $[t,\ L]$ pertence a $\mathcal{L}$.

   (a) Escreva todas as listas pertencentes a $\mathcal{L}$ de comprimento menor ou igual a 4.

(b) Quantas listas de comprimento 12 terá o conjunto $\mathcal{L}$? Justifique sucintamente.

(c) O mesmo que em (b) para um dado comprimento n.

2. Seja $\mathcal{L}$ o conjunto de todas as listas sobre $\{a,\ b\}$ que alternam a's e b's, como acontece, por exemplo, nas listas $[\,]$, $[a]$, $[b]$, $[a,b]$, $[b,a]$, $[a,b,a]$, $[b,a,b]$, $[a,b,a,b]$, ... Dê uma definição recursiva de todas as listas de $\mathcal{L}$.

6 Strings

Uma *string* é uma sequência finita de zero ou mais elementos colocados um a seguir ao outro por justaposição. Os elementos individuais com os quais podemos construir *strings* ou *palavras* constituem o *alfabeto*. Por exemplo,

$$aacabb$$

é uma *string* no alfabeto $\{a,b,c\}$. Uma *string* sem elementos diz-se *string vazia* e denota-se por Λ.

O número de elementos que aparecem numa *string* S diz-se *comprimento de* S e denota-se por $|S|$. Por exemplo, a *string* $aacabb$, no alfabeto $\{a,b,c\}$, tem comprimento 6.

Podemos considerar uma operação entre strings, dita *concatenação* e usualmente indicada por um ponto, $\cdot$, que consiste em justapôr duas *strings* pela ordem dada. Por exemplo, a concatenação de cb com aba dá $cbaba$, ou seja, $cb \cdot aba = cbaba$.

A concatenação é associativa, i.e., para quaisquer *strings* R, S e T num alfabeto A, verifica-se $(R \cdot S) \cdot T = R \cdot (S \cdot T)$.

A *string vazia* é elemento neutro da concatenação, i.e., para qualquer *string* S, verifica-se $\Lambda \cdot S = S \cdot \Lambda = S$.

Para um número natural n e uma *string* S, pode denotar-se por S^n a *string* $S \cdot S \cdot ... \cdot S$, onde S é repetida n vezes. Por exemplo, se a é um elemento do alfabeto, $a^0 = \Lambda$, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$.

Dado um alfabeto A, designamos por A^* o conjunto de todas as *strings* sobre o alfabeto A.

Definição recursiva de strings sobre um alfabeto A:

1. $\Lambda \in A^*$.

2. Se $a \in A$ e $S \in A^*$, então $a \cdot S \in A^*$.

6.1 Exercícios.

1. Defina recursivamente o conjunto L de *strings* sobre o alfabeto $A = \{0, 1\}$ que contêm exactamente uma ocorrência do elemento 0 sendo essa ocorrência na extremidade direita. (Assim são elementos de L, por exemplo, 0, 10, 110, 1110, ...)

2. Seja $A = \{0, 1\}$ e Q o conjunto de *strings* sobre A com a propriedade seguinte: Nenhuma *string* contém 0 na extremidade esquerda excepto o próprio 0. Defina Q recursivamente. (São elementos de Q, por exemplo, 0, 1, 10, 11, 100, 101, 110, ...)

3. Defina recursivamente o conjunto de todas as *strings* de comprimento par sobre um alfabeto A.

4. Construa uma definição recursiva do conjunto S de todas as *strings* sobre o alfabeto $\{a, b\}$, tal que
$$S = \{a,\ b,\ ab,\ ba,\ aab,\ bba,\ aaabb,\ bbba,\ ...\}\,.$$

5. Defina recursivamente o conjunto $\mathcal{L}$ de todas as strings sobre $B = \{0,\ 1\}$ da forma Λ, 01, $0011, 000111$, ..., isto é, as *strings* constituídas por um certo número de 0's consecutivos seguidos pelo mesmo número de 1's consecutivos.

6. Defina *strings* da forma $a^m b a^m$ recursivamente. Use a formação de regras para provar que todas as *strings* geradas desta maneira têm um número ímpar de caracteres.

7. Defina recursivamente o conjunto $\mathcal{L}$ de todas as *strings* sobre $B = \{0,\ 1\}$ que alternam 0's e 1's, como acontece, por exemplo, nas *strings* Λ, 0, $1, 01$, 10, 010, 1010, 01010, ...

8. Identifique as *strings* que pertencem ao conjunto A de *bit strings* definido recursivamente por

   $\Lambda \in A$

   $0x1 \in A$ se $x \in A$.

7 G-sequências, sequências decrescentes

Se G é um predicado de aridade 2 interpretado num domínio D, uma *G-sequência em D* é uma sequência tal que, para cada dois termos sucessivos x e y da sequência, $G(x, y)$ verifica-se.

7.1 Exemplos.

1. No domínio dos números inteiros, seja $G(x, y) := x > y$. Então toda a sequência (estritamente) decrescente é uma G-sequência. Assim, como exemplo de G-sequências

temos:

$$15,\ 5,\ 0$$
$$22,\ 21,\ 20,\ 19$$
$$-2,\ -4,\ -6,\ -9$$

2. Analogamente, para a mesma interpretação de G no domínio dos racionais, um exemplo é
$$1,\ 1/2,\ 1/4,\ 1/5,\ 1/6$$

3. Se considerarmos o domínio das fbf's no cálculo proposicional e G como a interpretação tal que $G(x, y)$ é verdadeiro se a fbf y entra na construção da fbf x, ou seja, y é uma subfórmula bem formada (própria) de x, então
$$(P \wedge Q) \wedge \neg R,\ P \wedge Q,\ P$$
é uma G-sequência.

Um domínio diz-se *bem-fundado* relativamente a um predicado G (de aridade 2) se todas as G-sequências têm fim.

Nos domínios bem-fundados existem elementos x tais que $G(x, y)$ é falsa para todo o y. Estes elementos dizem-se *minimais*.

O domínio dos números naturais (relativamente a ¿) tem apenas um elementos minimal, o 0.

Os elementos minimais no domínio das SL-expressões (relativamente a $G(x, y) := y$ é subexpressão própria de x) são as expressões atómicas.

Nos domínios cujos elementos são definidos recursivamente, podemos considerar G tal que $G(x, y)$ significa y é necessário para gerar x (ou seja, y entra na construção de x).

7.2 Exercícios.

1. Mostre que se $G(x, x)$ é verdadeiro então existem G-sequências infinitas.

2. Mostre que se existe um valor y tal que $G(x, y)$ e $G(y, x)$ são ambos verdadeiros então existem G-sequências infinitas.

8 Demonstrações por recursão

Seja D um domínio bem-fundado relativamente a um predicado G. Para provar que uma determinada propriedade $P(x)$ se verifica para todo o x de D podemos usar uma demonstração por recursão, cujos passos se descrevem a seguir:

Base indutiva: Mostra-se que a propriedade $P(x)$ é verdadeira para todo o elemento minimal x.

Hipótese indutiva: Supõe-se que, para dado x, $P(y)$ é verdadeira para todo o y tal que $G(x, y)$ se verifica.

Passo indutivo: Prova-se $P(x)$.

Conclusão: Conclui-se que $\forall x P(x)$.

8.1 Exemplo. O domínio $\mathbb{Z}$ não é bem-fundado relativamente a G tal que $G(x, y)$ significa que $x > y$. Logo não se podem fazer demonstrações por recursão neste domínio.

Mas claro que o domínio $\mathbb{N}$ é bem-fundado relativamente ao mesmo G. A chamada indução matemática forte não é mais do que uma demonstração recursiva no domínio dos naturais relativamente a $>$.

8.2 Exemplo. Pretende saber-se se o seguinte procedimento que leva ao cálculo de fact(n) termina sempre:

```
function fact(n: integer) : integer;
    begin
        if n=0 then fact:=1
        else fact:=n*fact(n-1);
    end;
```

É fácil concluir que termina se n é um inteiro não negativo. Mas não termina no caso de n ser qualquer inteiro.

Prova de que termina para $n \geq 0$:

Seja $P(n)$ verdadeiro se e só se fact(n) termina.

Domínio bem-fundado: O domínio dos números naturais é bem-fundado para o predicado $>$. Tem um só elemento minimal, 0.

Base indutiva: O programa termina para $n = 0$, logo $P(0)$ verifica-se.

Hipótese indutiva: Supõe-se que o programa termina para todos os $m < n$.

Passo indutivo: Por hipótese indutiva, fact(m) termina para todos os $m < n$. Em particular, fact(n-1) atingirá um valor e, então, no passo seguinte, o cálculo de fact(n) estará terminado.

Conclusão: Conclui-se que o valor de fact(n) é sempre atingido para todo o $n \geq 0$.

Se considerarmos n um número inteiro, a demonstração já não é válida, porque há sequências decrescentes infinitas no domínio dos inteiros. Nomeadamente, se $n = -1$, para calcular fact(-1), é preciso calcular fact(-2); para calcular fact(-2), é preciso calcular fact(-3); e assim sucessivamente pelo que o programa nunca mais acaba.

Quando definimos recursivamente os elementos de um dado conjunto, as regras recursivas podem ser *alongadoras* ou *encurtadoras*. Uma regra recursiva diz-se alongadora se o novo objecto a ser definido contém propriamente as componentes usadas na sua definição. Em todos os exemplos dados até aqui as regras recursivas eram alongadoras. As regras encurtadoras obtêm-se fazendo desaparecer algumas das componentes usadas na definição. É exemplo de regra encurtadora a seguinte:

"Se (A) é uma SL-expressão então A é uma SL-expressão."

Consideremos a seguinte definição recursiva de teorema:

1. Toda a premissa é um teorema.
2. Toda a expressão que pode ser deduzida de um teorema por meio de uma regra de inferência válida é um teorema.

Um exemplo de regra do tipo 2 é a seguinte: " De A e de $A \to B$ deduz-se B."
Esta regra é claramente encurtadora. As regras de inferência surgem assim como regras recursivas e, usualmente, existem regras encurtadoras e regras alongadoras entre as regras de inferência.

Já vimos atrás que nos domínios cujos elementos são definidos recursivamente, se pode considerar G tal que $G(x, y)$ significa y é necessário para gerar x (ou seja, y entra na construção de x, ou ainda, y é uma componente (própria) de x). Se todas as regras recursivas são alongadoras então todas as G-sequências terminam e os elementos minimais são os *elementos básicos*. Neste caso, o domínio é bem-fundado relativamente a G. A demonstração por recursão de uma propriedade $P(x)$ para todos os elementos do domínio, também chamada *Indução Estrutural*, pode neste caso ser descrita como a seguir:

Base indutiva: Prova-se que para todo o objecto básico x, $P(x)$ é verdadeiro.

Hipótese indutiva: Supõe-se que, para dado x, $P(y)$ é verdadeiro para todas as componentes próprias y de x.

Passo indutivo: Prova-se $P(x)$.

Conclusão: Conclui-se que $\forall x P(x)$.

8.3 Exemplo. Dual de uma SL-expressão C é a SL-expressão definida por:
dual(C)=dual(A)$\vee$ dual(B), se $C = A \wedge B$
dual(C)=dual(A)$\vee$ dual(B), se $C = A \vee B$
dual(C)=$\neg$dual(A) se $C = \neg A$
dual(C)=C, nos outros casos

Vamos provar, usando indução estrutural, que dual(C) se obtém de C substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$.

Seja $P(C)$ a propriedade "dual(C) obtém-se de C substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$". Vamos mostrar que $\forall C P(C)$:

Base indutiva: Se C é uma SL-expressão básica então não contém conectivos lógicos; logo, por definição de dual, fica dual(C)=C e é claro que se verifica $P(C)$.

Hipótese indutiva: Supõe-se $P(X)$ verdadeira para todo o X que é uma subexpressão própria de C.

Passo indutivo: Têm de ser considerados três casos:
1) $C = A \wedge B$: dual(C)=dual(A)$\vee$ dual(B) e, por hipótese indutiva, dual(A) e dual(B) obtêm-se de A e B, substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$. Logo dual(C) obtém-se de C substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$.
2) $C = A \vee B$: argumenta-se de forma análoga ao feito para 1).
3) $C = \neg A$: a hipótese indutiva, assegura que a SL-expressão A e, portanto, também a SL-expressão $\neg A$ se obtém de A substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$.

Conclusão: Para todo o C, dual(C) obtém-se de C substituindo todos os $\wedge$ por $\vee$ e todos os $\vee$ por $\wedge$.

8.4 Exercício. Complemento de uma SL-expressão C é a SL-expressão definida por:
comp(C)=comp(A)$\vee$comp(B), se $C = A \wedge B$
comp (C)=comp(A)$\wedge$ comp(B), se $C = A \vee B$
comp (C)= $\neg$comp(A) se $C = \neg A$ e A é composta
comp(C)=P se $C = \neg P$ e P é atómica
comp(C)= $\neg P$, se $C = P$ e P é atómica
Mostre que comp(C) $\equiv \neg C$.

8.5 Exercícios.

1. Defina E-expressões do seguinte modo:

   1. 2,3,4,... é uma E-expressão. A estas E- expressões chamamos atómicas.

   2. Se x e y são E-expressões, também o são $(x + y)$ e $(x \times y)$.

   E-expressões podem ser calculadas da forma habitual. Mostre que o valor de cada E-expressão é não inferior a $2n$, onde n é o número de expressões atómicas.

2. Dê uma definição recursiva de

   (a) todos os inteiros positivos múltiplos de 5;

(b) todos os inteiros positivos ímpares;

(c) todos os polinómios em x de coeficientes inteiros,

(d) todos os inteiros positivos congruentes com 2 módulo 3.

9 Sobre árvores

Definição (recursiva) do <u>nível de um vértice</u> de uma árvore:

1. Uma raiz tem nível 1.
2. O filho de um vértice de nível n tem nível $n + 1$.

A <u>altura de uma árvore</u> é o máximo de todos os níveis de vértces da árvore. A árvore vazia tem altura 0.

9.1 Teorema. *O número máximo de vértices de uma árvore binária de altura n é de $2n - 1$ e existe uma árvore binária de altura n com $2n - 1$ vértices.*

Demonstração. (Usando indução estrutural)

Base indutiva: A árvore vazia tem altura 0 e 0 vértices; como $2^0 - 1 = 0$, a propriedade verifica-se para a árvore vazia.

Hipótese indutiva: Suponhamos a propriedade válida para todas as subárvores próprias de uma árvore binária T de altura n.

Passo indutivo: Uma subárvore própria de uma árvore binária T de altura n pode ter quando muito altura $n - 1$ e, por hipótese indutiva, não pode ter mais do que $2^{n-1} - 1$ vértices. Como a árvore T é constituída por duas subárvores e pela raiz, os vértices de T são os das duas subárvores e a raiz, ou seja, não são mais do que $2(2^{n-1} - 1) + 1 = 2^n - 2 + 1 = 2^n - 1$.

Conclusão: O número máximo de vértices de uma árvore binária de altura n é $2n - 1$.

9.2 Exercício. Mostrar usando indução sobre n, que para todo o n existe uma árvore binária de altura n com exactamente $2^n - 1$ vértices.

9.3 Teorema. *Uma árvore binária não vazia de n vértices tem exactamente $n + 1$ subárvores vazias.*

Demonstração. (Usando indução estrutural)

Base indutiva: Uma árvore com 1 vértice tem 2=1+1 subárvores vazias.

Hipótese indutiva: Supõe-se que a propriedade é válida para todas as subárvores próprias de uma dada árvore T com n vértices. Isto significa que toda a subárvore própria não vazia de T com m vértices tem exactamente $m + 1$ subárvores vazias.

Passo indutivo: T é da forma (A, c, B). Se uma das subárvores A ou B é vazia, então a outra tem $n-1$ vértices e, por hipótese indutiva, tem n subárvores vazias. Portanto, T tem $n+1$ subárvores vazias. Se ambas as subárvores A e B são não vazias, sejam m_1 e m_2 o número de vértices de A e B, respectivamente. Então $n = m_1 + m_2 + 1$ e, por hipótese indutiva, A tem $m_1 + 1$ subárvores vazias e B tem $m_2 + 1$ subárvores vazias. Consequentemente T tem $(m_1 + 1) + (m_2 + 1) = n + 1$ subárvores vazias.

Conclusão: Todas as árvores binárias não vazias com n vértices têm exactamente $n+1$ subárvores vazias.

10 Funções definidas recursivamente

10.1 Exemplo.

1. A *sucessão de Fibonacci* define-se recursivamente por

    1. $f_0 = 0$; $f_1 = 1$;

    2. $f_n = f_{n-1} + f_{n-2}$, para $n \geq 2$.

2. A função $f(n) = a^n$, para $n \geq 0$, pode defenir-se por

    1. $f(0) = 1$;

    2. $f(n+1) = a \cdot f(n)$.

Para definir uma função f de aridade d por recursão primitiva, procede-se do seguinte modo:

Selecciona-se primeiro uma variável, por exemplo, x_d, como *variável recursiva*.

A definição consiste nas partes básica e recursiva, tendo-se:

Parte básica: $f(x_1, x_2, ..., 0) = e_0$

Parte recursiva: $f(x_1, x_2, ..., s(x_d)) = e_r$

e_0 tem de ser uma expressão não contendo f; nem e_0 nem e_r podem conter outras funções que ainda não estejam definidas.

10.2 Exemplos.

1. Definição recursiva primitiva da função *add* da adição de números naturais:

$$add(x, 0) = x$$
$$add(x, s(y)) = s(add(x, y))$$

2. Definição recursiva primitiva da <u>função predecessor</u>:

$$p(0) = 0$$
$$p(s(x)) = x$$

3. <u>Função subtracção própria</u>: A subtração própria entre x e y define-se por

$$x \dot{-} y = \begin{cases} x - y & \text{se } x > y \\ 0 & \text{se } x \leq y \end{cases}$$

   Uma definição recursiva da subtração própria é:

$$x \dot{-} 0 = x$$
$$x \dot{-} s(y) = p(x \dot{-} y)$$

4. Definição recursiva da <u>função sinal</u>:

$$sg(0) = 0$$
$$sg(s(x)) = 1$$

5. Definição recursiva da <u>função sinal inversa</u>:

$$isg(0) = 1$$
$$isg(s(x)) = 0$$

6. <u>Funções booleanas</u>:

$$and(p, q) = sg(p \times q)$$

$$or(p, q) = sg(p + q)$$

$$not(p) = isg(p)$$

7. <u>Função if</u>: A função if é dada por

$$if(x, y, z) = \begin{cases} y & \text{se } x > 0 \\ z & \text{se } x = 0 \end{cases}$$

   Portanto,

$$if(x, y, z) = (y \times sg(x)) + (z \times isg(x))$$

10.3 Exercícios.

1. Considere a seguinte função de Pascal:

```
function power(n:integer):integer;
  begin
    if n=0 then power:=1
    else power := 2*power(n-1)
  end
```

   Demonstre que esta função calcula 2^n para $n \geq 0$. Pode a demonstração ser generalizada para todos os valores inteiros de n?

2. Considere uma função $f : \mathbb{N} \to \mathbb{R}$ definida recursivamente por

   Base: $f(0) = f(1) = 1$;
   Regra recursiva: $f(n) = f(n-2) + f(n-1)$, para $n \geq 2$.

   Calcule os $f(k)$ para $k \leq 7$.

3. Determine $f(1)$, $f(2)$, $f(3)$ e $f(4)$ para $f(n)$ definida recursivamente por $f(0) = 1$ e, para $n = 0, 1, 2, ...$,

   (a) $f(n+1) = f(n) + 2$;
   (b) $f(n+1) = 2^{f(n)}$;
   (c) $f(n+1) = f(n)^2 + f(n) + 1$.

4. Determine $f(2)$, $f(3)$, $f(4)$ e $f(5)$ para $f(n)$ definida recursivamente por $f(0) = -1$, $f(1) = 2$ e, para $n = 1, 2, ...$,

   (a) $f(n+1) = f(n) + 3f(n-1)$;
   (b) $f(n+1) = f(n)^2 f(n-1)$;
   (c) $f(n+1) = f(n-1)/f(n)$.

5. A função de Conway é definida recursivamente por:

   f(1)=f(2)=1
   f(n)=f(f(n-1))+f(n-f(n-1)), para $n > 2$.

   Calcule $f(k)$ para $1 \leq k \leq 9$.

6. Dê uma definição recursiva da sucessão (a_n), $n = 1, 2, ...,$ se

   (a) $a_n = 6n$; (b) $a_n = 1+(-1)^n$; (c) $a_n = n(n+1)$; (d) $a_n = n^2$.

7. Seja F a função tal que $F(n)$ é a soma dos primeiros n inteiros positivos. Dê uma¡definição recursiva de $F(n)$.

8. Dê uma definição recursiva de $S_m(n)$, a soma do inteiro m com o inteiro não negativo n.

9. Dê uma definição recursiva de $P_m(n)$, o produto do inteiro m pelo inteiro não negativo n.

10. Os números de Fibonacci, f_0, f_1, f_2, ..., definem-se por

    $f_0 = 0$; $f_1 = 1$; $f_n = f_{n-1} + f_{n-2}$ para $n = 2, 3, 4, ...$

    (a) Calcule os números de Fibonacci f_2, f_3, f_4 e f_5.

    (b) Prove que $f_1^2 + f_2^2 + ... + f_n^2 = f_n f_{n+1}$ para todo $n \geq 1$.

    (c) Prove que $f_1 + f_3 + ... + f_{2n-1} = f_{2n}$ para todo $n \geq 1$.

    (d) (*) Prove que $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ para todo $n \geq 1$.

11. Seja $f(n) = 0 + 1 + ... + n$. Expresse $f(n)$ como uma função recursiva primitiva. Assuma que $s(n)$ e $add(n, m)$ são as únicas funções dadas.

12. Expresse a multiplicação de inteiros em termos de funções recursivas primitivas. Para isso, represente cada factor pelo seu sinal e o seu valor absoluto.

13. Seja $H(0) = 0$ e $H(n + 1) = 2 + H(n)$. Será $H(n)$ uma função recursiva primitiva?

14. O programa seguinte calcula c usando a como input. Expresse c como uma função de a.

```
b:=3+a;
c:=2+a;
c:=c*b;
```

15. Expresse o valor final da variável soma *sum* como uma função recursiva primitiva.

```
for i:=1 to n do sum:=sum+i*i
```

16. Use a função **if** para exprimir $f(n) = n$ mod3 na forma de uma função recursiva primitiva.

17. Mostre que a seguinte função g calcula correctamente o maior divisor comum entre cada par de inteiros positivos x e y:

$$g(x,y) = \begin{array}{l} \text{if } x = y \text{ then } x \\ \text{else if } x > y \text{ then } g(x-y,y) \\ \text{else } g(x, y-x). \end{array}$$

18. Use indução matemática para provar que uma função F definida especificando $F(0)$ e a regra para obter $F(n+1)$ de $F(n)$ está bem-definida.

19. Use indução matemática (forte) para provar que uma função F definida especificando $F(0)$ e a regra para obter $F(n+1)$ de $F(k)$ para $k \leq n$ está bem-definida.

20. Mostre que cada uma das definições recursivas de uma função no conjunto dos inteiros positivos propostas a seguir não estão correctas.

    (a) $F(1) = 1$ e $F(n) = 1 + F([n/2])$ para $n \geq 1$.

    (b) $F(1) = 2$, $F(2) = 3$ e $F(n) = 1 + F(n-3)$ para $n \geq 3$.

    (c) $F(1) = 1$, $F(2) = 2$ e $F(n) = 1 + F(n/2)$ para $n \geq 2$.

    (d) $F(n) = 1 + F(F(n-1))$ se $n \geq 2$ e $F(1) = 2$.

11 Exercícios

1. Considere o conjunto $A = \{c, a, b, o\}$.

    (a) Determine o número de listas de elementos de A de comprimento três cuja cabeça é uma vogal.

    (b) Seja $\mathcal{W}$ o conjunto de todas as *strings* sobre o alfabeto A definidas recursivamente por:

    (i) a e o pertencem a $\mathcal{W}$.

    (ii) Se $S \in \mathcal{W}$ e S começa por uma vogal então $b \cdot S$ e $c \cdot S$ pertencem a $\mathcal{W}$. Se $S \in \mathcal{W}$ e S começa por uma consoante então $a \cdot S$ e $o \cdot S$ pertencem a $\mathcal{W}$.

    Apresente todas as *strings* de $\mathcal{W}$ de comprimento menor ou igual a 3.

    Quantas das strings de $\mathcal{W}$ têm comprimento 4? E 5?

    (c) Defina recursivamente o conjunto de todas as árvores binárias sobre A tais que cada nodo com filho tem ou dois filhos etiquetados por duas vogais ou dois filhos etiquetados por duas consoantes.

2. Use indução matemática para provar que todo o $n \geq 0$ verifica a igualdade

$$\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!} \ .$$

3. Prove por indução que, para todo o $n \geq 0$, se verifica a igualdade: $\displaystyle\sum_{i=1}^{n}(i^2 - i) = \frac{n(n^2-1)}{3}$.

4. (a) Defina nível de um vértice e altura de uma árvore binária.

   (b) A seguir está escrita a demonstração de que dado um conjunto $X \neq \emptyset$, para todo o natural n existe uma árvore binária sobre X de altura n com exactamente $2^n - 1$ vértices. Complete a demonstração escrevendo na sua folha de prova o correspondente a (A) e a (B).

   Demonstração. A propriedade é válida para $n = 0$, visto que a árvore vazia $\overset{(A)}{\ldots\ldots\ldots}$.

   Suponhamos a propriedade válida para n. Vamos mostrar que então também se verifica para $n + 1$. Com efeito, por hipótese indutiva, existe uma árvore binária A de altura n e com exactamente $2^n - 1$ vértices. Seja $T = (A, x, A)$, com $x \in X$. Então a altura de T é igual a 1 somado à altura de A, ou seja, $n + 1$. Por outro lado, denotando por $v(T)$ o número de vértices de T e por $v(A)$ o número de vértices de A, tem-se $\overset{(B)}{\ldots\ldots\ldots}$.

5. Seja $\mathcal{T}$ um conjunto de árvores binárias sobre o conjunto $A = \{0, 1\}$ cujas árvores de altura menor ou igual a 3 são $A = (0)$, $B = (1)$, $C = ((1), 0, (1))$, $D = ((0), 1, (0))$, $E = (((0), 1, (0)),\ 0,\ ((0), 1, (0)))$ e $F = (((1), 0, (1)),\ 1,\ ((1), 0, (1)))$.

   (a) Desenhe as árvores A, B, C, D, E e F.

   (b) Sabendo que $\mathcal{T}$ tem todas as árvores de qualquer altura que se formam por um processo análogo ao exposto nos exemplos dados, dê uma definição recursiva de $\mathcal{T}$.

6. Seja f a função de variável natural definida para $n \geq 1$ por $f(n) = \dfrac{(n-1)!}{2^n}$.

   (a) Determine $f(1)$, $f(2)$, $f(3)$ e $f(4)$.

   (b) Dê uma definição recursiva de f.

7. (a) Mostre que $n^2 + n$ é um número par para todo o número natural n.

(b) Use indução matemática para provar que 6 divide $n^3 - n$ para todo o $n \geq 0$.

8. (a) Defina cabeça e cauda de uma lista. Defina recursivamente lista sobre um conjunto A.

   (b) Defina recursivamente todas as listas não vazias sobre o conjunto $\{x, y, z\}$ tais que a a letra x aparece sempre com outro x ao lado; por exemplo, $[y]$, $[y, z]$, $[x, x]$, $[x, x, x]$, $[y, x, x, z, y]$, $[z, x, x, y, x, x, z, z]$.

   (c) Determine o número de listas de comprimento 4 da forma descrita na alínea anterior.

9. Seja $\mathcal{T}$ o conjunto de todas as árvores binárias não vazias sobre o conjunto $\{a, b\}$ tais que cada vértice com filhos tem dois filhos iguais. Dê uma definição recursiva de $\mathcal{T}$.

10. Considere o conjunto $\mathcal{S}$ de todas as strings sobre o conjunto $\{0, 1\}$ definido recursivamente por:

    1. A string vazia pertence a $\mathcal{S}$.

    2. Se S pertence a $\mathcal{S}$ então a string $S \cdot 0$ pertence a $\mathcal{S}$. Se S pertence a $\mathcal{S}$ e S não termina em 1 então a string $S \cdot 1$ pertence a $\mathcal{S}$.

    (a) Apresente todas as strings pertencentes a $\mathcal{S}$ de comprimento 2 e 3.

    (b) Mostre que a função f definida recursivamente por
    $f(0) = 1,\ f(1) = 2;$
    $f(n) = f(n-1) + f(n-2),\ \text{para } n \geq 2$
    verifica a igualdade $f(n+1) = 2f(n-1) + f(n-2)$, para todo o $n \geq 2$.

    (c) Considere a afirmação $P(n)$ indicada a seguir:
    $P(n)$:="O número de strings pertencentes a $\mathcal{S}$ de comprimento n é igual a $f(n)$, sendo $f(n-1)$ delas a terminar em 0 e as restantes $f(n-2)$ a terminar em 1."
    onde f é a função da alínea anterior.
    Prove que a propriedade $P(n)$ é verdadeira para todo o $n \geq 2$.

11. (a) Prove por indução que para todo o $n \geq 0$, $\displaystyle\sum_{k=1}^{n}(2k+1) = n^2$.

    (b) Use o resultado da alínea anterior para calcular a soma de todos os números ímpares positivos menores do que 122.

12. (a) Represente graficamente as árvores binárias $A = ((b), a, ((a), b, (a)))$ e $B = (((a), b, (a)), b, ((b), b, (b)))$.

    (b) Defina recursivamente árvore binária sobre um conjunto X.

(c) Seja $\mathcal{T}$ o conjunto das árvores binárias sobre o conjunto $\{0, 1\}$ definidas recursivamente por:

1. (0) e (1) pertencem a $\mathcal{T}$.
2. Se A é uma árvore em $\mathcal{T}$ de raiz 0 e B é uma árvore em $\mathcal{T}$ de raiz 1, então $(A, 0, B)$ e $(B, 1, A)$ pertencem a $\mathcal{T}$.

Represente todas as árvores de $\mathcal{T}$ de altura menor ou igual a 3.

(d) Seja $\mathcal{U}$ o conjunto de todas as árvores binárias não vazias sobre o conjunto $\{a, b\}$ tais que cada vértice com filhos tem dois filhos iguais (como acontece, por exemplo, com as árvores A e B da alínea (a)). Dê uma definição recursiva de $\mathcal{U}$.

Capítulo V

GRAFOS

1 Definições básicas

Um grafo é constituído por um conjunto finito de vértices e um conjunto finito de arcos (ou arestas) que ligam pares de vértices. O diagrama da Figura 1 representa um grafo com 4 vértices e 6 arestas. Mais precisamente: Um *grafo* $G = (V, E, f)$ é constituído por

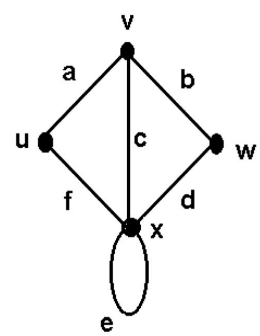


Figura 1: grafo

um conjunto não vazio V chamado o conjunto dos *vértices* (ou *pontos* ou *nodos* ou *nós*) do grafo, um conjunto E dito o conjunto das *arestas* (ou *arcos*) do grafo, uma função f do conjunto E das arestas para um conjunto de pares ordenados ou não ordenados de vértices. Se uma aresta tem como imagem um par ordenado, diz-se uma *aresta dirigida*; caso contrário , diz-se uma *aresta não dirigida*.

Se uma aresta $a \in E$ está associada a um par ordenado (u, v) ou a um par não ordenado $\{u, v\}$, onde $u, v \in V$, dizemos que a liga os vértices u e v.

Dois vértices ligados por uma aresta dizem-se *adjacentes*. Um vértice que não é adjacente a nenhum outro diz-se *isolado*.

Por vezes representa-se um grafo apenas por G ou por (V, E).

Um grafo no qual todas as aresta são dirigidas diz-se um *grafo dirigido* ou *digrafo*.
Um grafo no qual todas as arestas são não dirigidas diz-se um *grafo não dirigido*.
Se tiver arestas dirigidas e arestas não dirigidas, diz-se *misto*.

Se $G = (V, E)$ é um grafo e a é uma aresta associada com o par ordenado (u, v), dizemos que que *a se inicia* (ou *tem origem*) em u e *acaba* (ou *termina*) em v. Dizemos também que a aresta é *incidente* em u e v.

Uma aresta que liga um vértice a si próprio diz-se *lacete*. O sentido de um lacete não é significativo, portanto um lacete pode ser considerado tanto dirigido como não dirigido.

Na Figura 1, o arco e é um lacete e os vértices u e v são adjacentes.

Na Figura 2 representam-se quatro grafos por meio de diagramas.

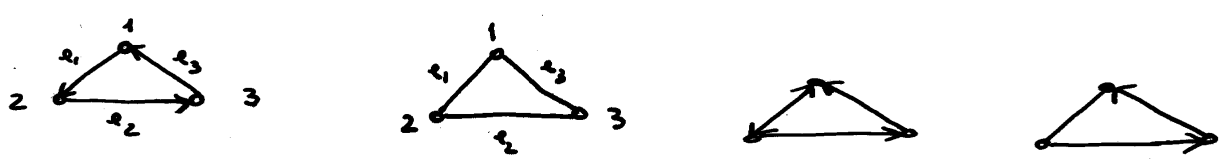


Figura 2: grafos

Podemos ter pares de vértices ligados por mais do que uma aresta. Tais arestas dizem-se *paralelas*. Nos primeiro e segundo grafos da Figura 3 há arestas paralelas mas não no terceiro.

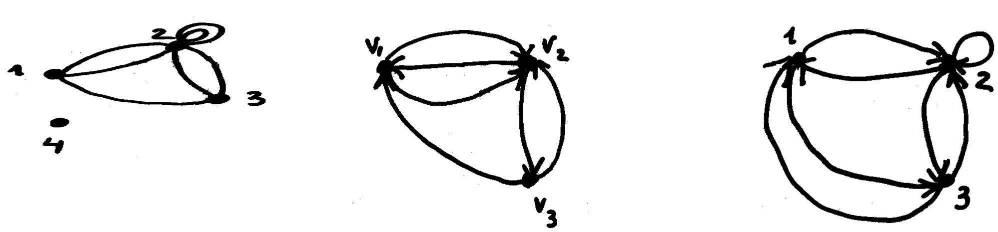


Figura 3: grafos

Um grafo que contenha algumas arestas paralelas diz-se *multigrafo*. Neste caso, a aplicação f entre arestas e pares de vértices não é injectiva. Por isso, quando se trata de um multigrafo não é conveniente usar a notação abreviada $G = (V, E)$ em vez da notação completa $G = (V, E, f)$.

Se num grafo não existir mais do que uma aresta entre cada par de vértices (não mais do que uma aresta dirigida em cada um dos sentidos, no caso de um grafo dirigido) e não tiver lacetes, diz-se um *grafo simples*. Vamos estudar sobretudo grafos simples e, a menos que seja especificado o contrário, quando falarmos de grafos, referir-nos-emos aos simples.

Num grafo dirigido, para cada nodo v, o número de arestas que têm v como nodo inicial diz-se o *grau fora* de v e o número de arestas que têm v como nodo terminal diz-se *grau dentro*. O *grau total* de v é a soma do grau fora com o grau dentro. Se o grafo for não dirigido o *grau total* ou apenas *grau* de v é igual ao número de arestas incidentes em v.

Sejam $G = (V_1, E_1)$ e $H = (V_2, E_2)$ dois grafos tais que $V_1 \subseteq V_2$ e $E_1 \subseteq E_2$. O grafo G diz-se um *subgrafo* do grafo H e escreve-se $G \subseteq H$. Na Figura 4, os grafos G, H, K e L são subgrafos de G.

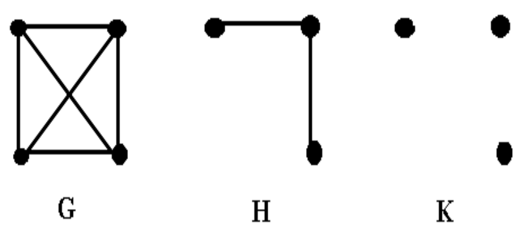


Figura 4: subgrafos

Um grafo (V, E) diz-se *completo* se cada vértice é adjacente a todos os outros vértices do grafo. Denotamos um grafo completo de n vértices por K_n. A Figura 5 representa K_n para $n = 1, 2, 3, 4, 5$.

Um grafo diz-se *bipartido* se o seu conjunto de vértices V pode ser particionado em subconjuntos V_1 e V_2 tais que os vértices de V_1 não são adjacentes entre si e o mesmo acontece com os vértices de V_2.

A Figura 6 representa um grafo bipartido.

Um *grafo não dirigido* pode ser considerado como um grafo dirigido se associarmos a cada aresta não dirigida $\{u, v\}$ duas arestas dirigidas, (u, v) e (v, u).

Se $G = (V, E)$ é um qualquer grafo sem arestas paralelas, E pode ser expresso como um conjunto de pares ordenados, logo $E \subseteq V \times V$ pode ser considerado como uma relação em

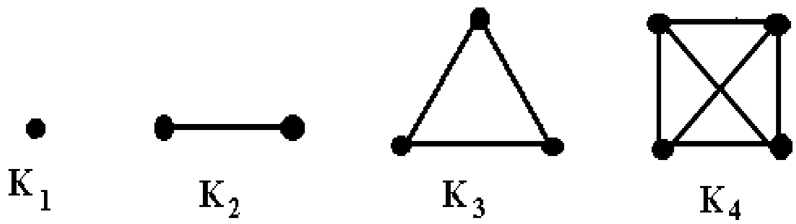


Figura 5: grafos completos

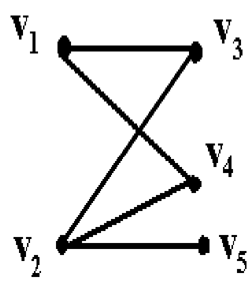


Figura 6: grafo bipartido

V. Assim dizemos que o grafo $G = (V, E)$ é *reflexivo*, *simétrico*, *anti-simétrico*, *transitivo*, etc., se a relação E o for. Um grafo não dirigido é simétrico. (Porquê?)

Isomorfismo de grafos. Dois grafos $G_1 = (V_1, A_1)$ e $G_2 = (V_2, A_2)$ dizem-se *isomorfos* se existir uma função bijectiva

$$\phi : V_1 \to V_2$$

tal que para quaisquer dois vértices u e v de V_1 se tem que

$$(u, v) \in A_1 \Leftrightarrow (\phi(u), \phi(v)) \in A_2 \quad \text{e} \quad \{u, v\} \in A_1 \Leftrightarrow \{\phi(u), \phi(v)\} \in A_2.$$

A função ϕ satisfazendo estas condições diz-se um isomorfismo de grafos e escrevemos $G_1 \simeq G_2$ para indicar que G_1 e G_2 são isomorfos.

Por outras palavras, ϕ é um isomorfismo entre G_1 e G_2 se $\phi : V_1 \to V_2$ for uma função bijectiva e a correspondência ϕ' dada por

$$(u, v) \mapsto (\phi(u), \phi(v))$$
$$\{u, v\} \mapsto \{\phi(u), \phi(v))\}$$

define também uma função bijectiva $\phi' : A_1 \to A_2$.

Como exemplo, consideremos os dois grafos da Figura 7.

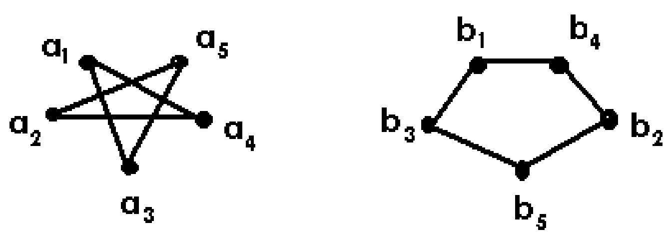


Figura 7: grafos isomorfos

Eles são isomorfos. Com efeito, se definirmos ϕ por

$$\phi(a_1) = b_1,\ \phi(a_2) = b_5,\ \phi(a_3) = b_4,\ \phi(a_4) = b_3,\ \phi(a_5) = b_2,$$

a correspondência ϕ' definida por $\phi'(\{x, y\}) = \{\phi(x),\ \phi(y)\}$, para cada aresta $\{x, y\}$ do primeiro grafo, é também uma função bijectiva.

1.1 Exercícios.

1. Desenhe o grafo $G = (V, E)$, onde $V = \{1, 2, 3, 4, 5\}$ e $E = \{\{1, 2\}, \{1, 3\}, \{1, 5\}, \{2, 3\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$. Determine o conjunto $W = \{i \,|\, i$ é um vértice tal que i e 2 são adjacentes$\}$.

2. Desenhe o grafo dirigido $G = (V, E)$, onde $V = \{1, 2, 3, 4, 5\}$ e $E = \{(1, 2), (1, 3), (1, 5), (2, 3), (5, 1), (5, 3), (4, 1), (4, 4)\}$.

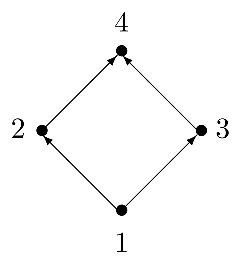
3. Construa um grafo completo com 4 vértices tal que os arcos não se intersectem. Construa um grafo completo com 5 vértices.

4. Desenhe os grafos K_3 e K_6.

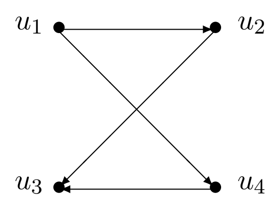
5. Mostre que: (a) um grafo não dirigido (simples) completo com n vértices tem o número máximo de arestas, isto é, $\dfrac{n(n-1)}{2}$; (b) um digrafo (simples) completo com n vértices tem o número máximo de arestas, isto é, $n(n-1)$.

6. Em cada uma das alíneas seguintes, mostre que os dois grafos dados são isomorfos.

(a)

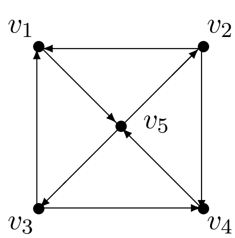


G

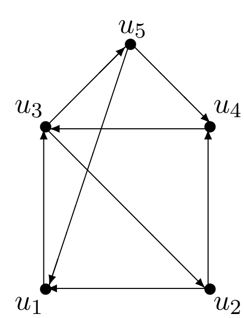


H

(b)



K



L

7. Mostre que o isomorfismo de grafos é uma relação de equivalência na classe de todos os grafos.

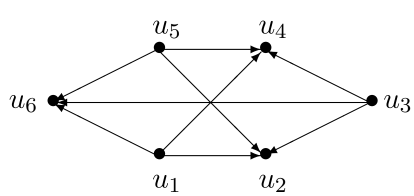
   Mostre que todos os grafos pertencentes à mesma classe de equivalência têm o mesmo número de vértices, o mesmo número de arestas e o mesmo número de vértices com um determinado grau. Descubra outras propriedades que sejam invariantes numa mesma classe de equivalência.

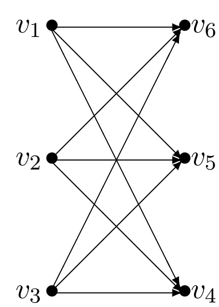
8. Desenhe todos os digrafos simples com três vértices, supondo que grafos isomorfos não se distinguem. Mostre que existe apenas

   - um tal digrafo sem arestas;
   - um com uma aresta;
   - quatro com duas arestas;
   - quatro com três arestas,
   - quatro com quatro arestas;
   - um com cinco arestas;
   - um com seis arestas.

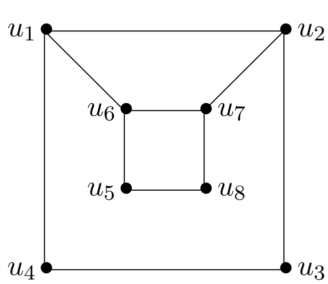
   Estabeleça as propriedades desses grafos no que respeita à simetria, transitividade, etc.

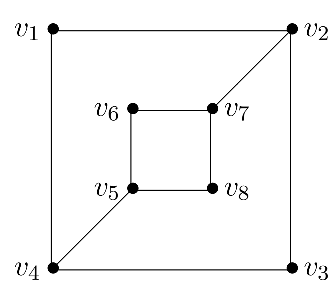
9. Mostre que os grafos seguintes são isomorfos.





10. Mostre que os grafos seguintes não são isomorfos.





2 Caminhos, ciclos e conexidade

Seja $G = (V, E)$ um digrafo simples. Um *caminho* em G é uma sequência de arestas tal que o vértice terminal de cada aresta é o vértice inicial da aresta seguinte na sequência.

Portanto,

$$< (v_1, v_2),\ (v_2, v_3),\ ...,\ (v_{k-2}, v_{k-1}),\ (v_{k-1}, v_k) >$$

é um caminho, supondo que todos os vértices e arestas que aparecem na sequência pertencem a V e a E, respectivamente. Usualmente representamos um tal caminho por

$$< v_1,\ v_2,\ v_3,\ ...,\ v_{k-2},\ v_{k-1},\ v_k > \ .$$

Claro que nem toda a sequência de vértices é um caminho.

O *caminho trivial* de v para v consiste num único vértice, $< v >$.

2.1 Exercícios. Faça o diagrama de um digrafo com cinco vértices e três arestas. Indique uma sequência de vértices que seja um caminho e uma outra que o não seja.

O número de arestas que aparecem num caminho diz-se o *comprimento do caminho*. Um caminho num digrafo no qual as arestas são todas distintas diz-se um *caminho simples*. Um caminho no qual todos os vértices são distintos diz-se um *caminho elementar*.

Relativamente ao digrafo da Figura 8, alguns dos caminhos de 1 para 9 são:

$$P_1 =< 1, 9 >$$
$$P_2 =< 1, 2, 3, 8, 1, 9 >$$
$$P_3 =< 1, 2, 4, 5, 7, 8, 1, 9 >$$

P_1, P_2 e P_3 são todos caminhos simples mas P_2 e P_3 não são elementares.

Um caminho não trivial da forma

$$< v_1,\ v_2,\ ...,\ v_n,\ v_1 > ,$$

que começa e acaba no mesmo vértice, diz-se um *ciclo*. Um ciclo diz-se *simples* se nenhuma aresta do ciclo aparecer mais do que uma vez e diz-se *elementar* se não passar por nenhum vértice mais do que uma vez, excepto no inicial e terminal. Um ciclo simples também se diz *circuito*.

Aluns ciclos do grafo da Figura 9 são:

$$C_1 =< 1, 2, 3, 8, 1 >$$
$$C_2 =< 1, 2, 4, 5, 7, 8, 1 >$$
$$C_3 =< 1, 2, 3, 8, 1, 2, 3, 8, 1 >$$

Um digrafo simples que não tem ciclos diz-se *acíclico*. A Figura 9 representa grafos acíclicos.

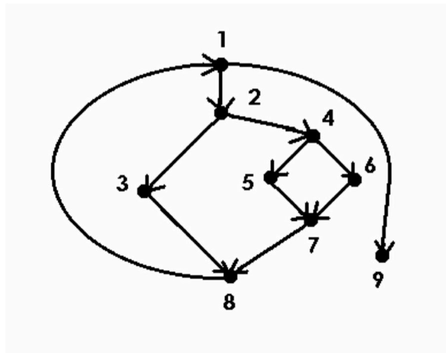


Figura 8: caminhos

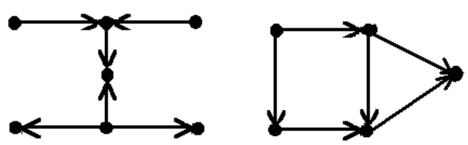


Figura 9: grafos acíclicos

Seja G um digrafo simples. Se u e v são dois vértices de G dizemos que v é *atingível* por u se $v = u$ ou se existir algum caminho de u para v.

Se um vértice v é atingível por um outro vértice u, um caminho de u para v com menor comprimento diz-se um *caminho de comprimento mínimo*. O comprimento dum caminho de comprimento mínimo diz-se a *distância de u a v* e denota-se por $d(u, v)$. Quando não existe nenhum caminho de u para v costuma escrever-se $d(u, v) = \infty$.

2.2 Exercícios.

1. Verificar que a distância $d(u, v)$ entre dois vértices de um digrafo tem as seguintes

propriedades:

$$d(u,u) = 0$$
$$d(u,v) \geq 0$$
$$d(u,v) + d(v,w) \geq d(u,w) \text{ (desigualdade triangular)}$$

Compare estas propriedades com as propriedades de outras distâncias que já conhece.

2. Dê um exemplo que mostre que

   (a) se pode ter $d(u,v) + d(v,w) > d(u,w)$;

   (b) se pode ter $d(u,v) \neq d(v,u)$.

2.3 Teorema. *Num digrafo simples, o comprimento de cada caminho elementar é menor ou igual a $n-1$, onde n é o número de vértices do grafo. Analogamente, o comprimento de cada ciclo elementar não excede n.*

Demonstração. A prova baseia-se no facto de que num caminho elementar cada vértice não aparece mais do que uma vez. Assim, o número de vértices distintos num caminho elementar de comprimento k é $k+1$. Como o grafo só tem n vértices distintos, não é possível arranjar um caminho elementar de comprimento maior do que $n-1$.

Para um ciclo elementar de comprimento k, a sequência dos vértices tem k distintos; pelo que, havendo no grafo não mais do que n vértices distintos, um ciclo elementar não pode exceder n em comprimento.

Até aqui falámos de caminhos e ciclos em grafos dirigidos. Vamos ver como estas noções se estendem a grafos não dirigidos.

As definições de caminho e ciclo e as definições e propriedades relacionadas que estudámos para grafos dirigidos são naturalmente estendidas aos *grafos não dirigidos*.

Por exemplo, num grafo não dirigido simples uma sequência

$$< v_1, v_2, ..., v_d >$$

constitui um caminho se para $i = 2, 3, ..., d$ existir uma aresta $\{v_{i-1}, v_i\}$ (dita aresta do caminho). O comprimento do caminho é dado pelo número de arestas do caminho, ou seja, $d-1$.

Um grafo não dirigido diz-se *acíclico* se não tiver ciclos simples (ou circuitos). Note-se que, ao contrário dos grafos dirigidos, um grafo não dirigido pode ter ciclos sem ter ciclos simples. Com efeito, se contiver a aresta $\{v_1, v_2\}$, então $< v_1, v_2, v_1 >$ é um ciclo que repete uma aresta.

Um grafo não dirigido diz-se *conexo* se for não vazio e cada dois vértices do grafo podem ser ligados por um caminho.

Dado um grafo $G = (V, E)$, considere-se em V a relação C definida por:

$$uCv \qquad \text{sse} \qquad \text{existe um caminho de } u \text{ para } v$$

Se G é não dirigido, a relação C em V é reflexiva, simétrica e transitiva. (Justifique.) Logo V pode ser particionado em classes de equivalência. G fica assim particionado em subgrafos que se dizem *componentes conexas* (ou apenas *componentes*) do grafo. O grafo da Figura 9 tem três componentes.

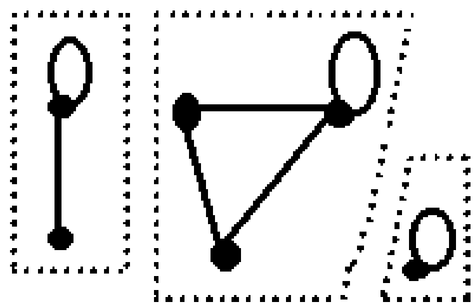


Figura 10: componentes

Dizemos que um digrafo é *conexo* (ou *fracamente conexo*) se o grafo não dirigido obtido desse digrafo considerando todas as suas arestas como sendo arestas não dirigidas for conexo. Na Figura 11, o grafo da esquerda é conexo, o da direita é desconexo, i.e., não é conexo.

Figura 11: digrafo conexo e digrafo não conexo

Um digrafo simples não vazio diz-se *unilateralmente conexo* se para cada par de vértices do grafo pelo menos um dos vértices do par é atingível pelo outro. Se para cada par de vértices cada um dos vértices é atingível pelo outro dizemos que o grafo é *fortemente conexo*.

2.4 Observação. É imediato que, para digrafos, se tem:

ser fortemente conexo $\Rightarrow$ ser unilateralmente conexo $\Rightarrow$ ser conexo

Relativamente aos digrafos da Figura 12, temos que o primeiro é fortemente conexo, o segundo é fracamente conexo mas não unilateralmente conexo, e o terceiro é unilateralmente conexo sem ser fortemente conexo. (Justifique.)

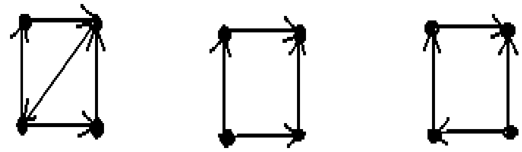


Figura 12: conexidade

Portanto, as implicações recíprocas das apresentadas na Observação acima não são verdadeiras.

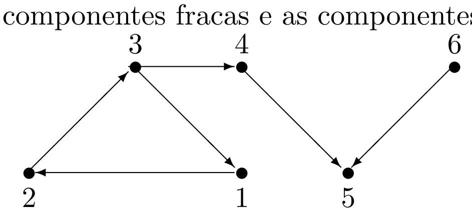
Seja $G = (V, E)$ um digrafo simples e $X \subseteq V$. Um subgrafo cujos vértices são os elementos de X e cujas arestas são as arestas de G que têm os seus vértices inicial e terminal em X diz-se um *subgrafo induzido por* X.

Um subgrafo G_1 diz-se *maximal* relativamente a uma dada propriedade se não existir nenhum outro subgrafo que tenha essa propriedade e contenha G_1.

Para um digrafo simples, um subgrafo fortemente conexo maximal diz-se uma *componente forte*.

Analogamente, um subgrafo unilateralmente conexo (respectivamente, fracamente conexo) maximal diz-se uma *componente unilateral* (respectivamente, *componente fraca*).

2.5 Exercício. Relativamente ao digrafo representado na figura a seguir, indique as componentes fortes, as componentes fracas e as componentes unilaterais.



2.6 Teorema. *Todo o vértice de um digrafo simples pertence a exactamente uma componente fraca.*

Demonstração. Atendendo à definição de conexidade fraca, para demonstrar o teorema basta prová-lo para um grafo não dirigido, ou seja, basta mostrar que cada vértice de um grafo não dirigido pertence a uma e só uma componente.

Seja então $H = (V, A)$ um grafo não dirigido.

Para cada vértice u do grafo H, sejam

$$C_u = \{v \in V : \text{existe um caminho de } u \text{ para } v\}$$

$$X_u = \text{subgrafo de } H \text{ induzido por } C_u.$$

Vamos mostrar que:

1) X_u é conexo;
2) X_u é maximal relativamente à propriedade de ser conexo;
3) $X_u \cap X_v \neq \emptyset$ implica que $X_u = X_v$.

Note-se que as propriedades 1) e 2) asseguram que X_u é uma componente conexa.

1) X_u é conexo: Sejam $v, w \in X_u$. Então existem caminhos
C_1 de u para v;
C_2 de u para w.
Como H é não dirigido, então também existe um caminho
C_1' de v para u.
Juntando os caminhos C_1' e C_2, obtemos um caminho de v para w.

2) X_u é maximal relativamente à propriedade de ser conexo:
Seja Y um sugrafo conexo de H que contém X_u. Vamos mostrar que $Y \subseteq X_u$.
Se $v \in Y$, como $u \in Y$ e Y é conexo, existe um caminho de u para v; mas então $v \in X_u$.

3) $X_u \cap X_v \neq \emptyset$ implica que $X_u = X_v$:
Se $w \in X_u \cap X_v \neq \emptyset$ então existem caminhos
C_1 de u para w;
C_2 de v para w.
Dado um qualquer vértice t de X_u, existe um caminho
C_3 de u para t.
Usando o caminho C_2, seguido do caminho inverso de C_1, seguido do caminho C_3, obtemos um caminho de v para t. Logo $t \in X_v$.

Concluimos assim que $X_u \subseteq X_v$. Analogamente se mostra que $X_v \subseteq X_u$.

2.7 Teorema. *Num digrafo simples $G = (V, E)$, todo o vértice do digrafo pertence a exactamente uma componente forte.*

Demonstração. Seja $v \in V$ e seja S o conjunto de todos os vértices u de G tais que existe um caminho de v para u e existe um caminho de u para v. É claro que $v \in S$ e, por outro lado, é fácil concluir que S é uma componente forte de V. Isto mostra que v pertence a uma componente forte S. Para mostrar que é a única, suponhamos que v pertence a outra componente forte, digamos, R. Mas então, para todo o vértice u de R, existem um caminho de u para v e um caminho de v para u. Isto implica que $u \in S$. Consequentemente, $R \subseteq S$. Mas R é uma componente forte, logo maximal, pelo que tem de ser $R = S$.

2.8 Observação. Pelos teoremas anteriores concluimos que tanto as as componentes fracas como as fortes determinam uma partição de V. De notar que o mesmo não acontece com as componentes unilaterais (veja o exercício anterior).

2.9 Ciclos de Euler.

A figura a seguir esquematiza as pontes de Königsberg.

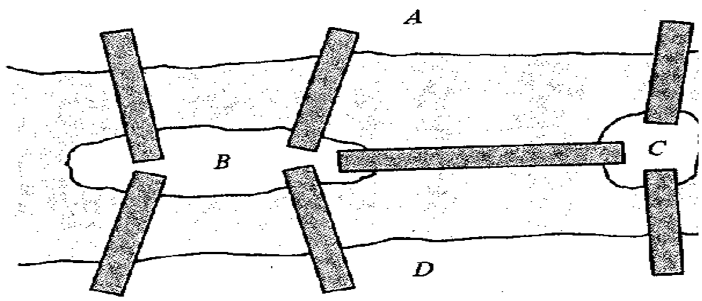


Figura 13: pontes de Königsberg

O problema das pontes de Königsberg foi estudado por Euler que apresentou a sua resolução num artigo de 1736. Duas ilhas no rio Pregel em Königsberg, na Rússia, estão ligadas entre si por uma ponte e as ilhas estão ligadas às margens por várias pontes como mostrado na Figura 13. O problema consiste em começar num dos pontos A, B, C ou D, caminhar sobre cada uma das pontes exactamente uma vez e acabar no ponto de partida.

Este problema pode formalizar-se do seguinte modo: Determinar se no grafo da Figura 14 existe algum ciclo simples que contenha todas as arestas do grafo.

Um ciclo num grafo G diz-se um *ciclo de Euler* se for simples e contiver todas as arestas e todos os vértices de G.

2.10 Teorema. *Um grafo G tem um ciclo de Euler se e só se for conexo e cada um dos seus vértices tiver grau par.*

2.11 Exercício. Qual é a resposta ao problema das pontes de Königsberg?

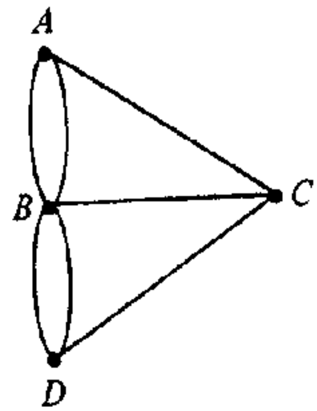


Figura 14: pontes de Königsberg

2.12 Exemplo do uso de digrafos simples para estudar o estado de utilização de recursos
de um sistema operativo.

Consideremos, num computador:

- o sistema do computador;
- vários programas que partilham os recursos do sistema;
- o sistema operativo.

Se um programa p_1 está a utilizar um recurso r_1, consideramos uma aresta de r_1 para p_1:

$$r_1 \bullet \longrightarrow \bullet\, p_1$$

Se p_1 precisa do recurso r_2, consideramos uma aresta de p_1 para r_2:

$$p_1 \bullet \longrightarrow \bullet\, r_2$$

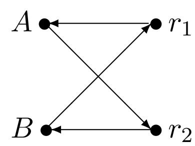
Podemos interpretar esta última aresta como o pedido do recurso r_2 pelo programa p_1.

Supõe-se que todos os pedidos de um recurso têm de ser satisfeitos para que possa ser completada a execução do programa. Se houver algum recurso indisponível o programa tem o controlo dos disponíveis mas tem de esperar pelo indisponível.

Num instante t, podemos considerar:

- o conjunto P_t dos programas em funcionamento no instante t;
- o conjunto R_t dos recursos;
- o grafo de ocupação G_t que representa o estado de ocupação dos recursos no instante t.

Se um programa A tem o control do recurso r_1 e requer o recurso r_2 mas o programa B tem o control de r_2 e requer r_1, como representado pelo grafo



o computador fica num estado de impasse. Temos um ciclo.

Por exemplo, sejam

$$R_t = \{r_1, r_2, r_3, r_4\} \quad \text{e} \quad P_t = \{p_1, p_2, p_3, p_4\}$$

e suponhamos que o estado de ocupação no instante t é o seguinte:

p_1 tem o recurso r_4 e requer r_1
p_2 tem o recurso r_1 e requer r_2 e r_3
p_3 tem o recurso r_2 e requer r_3
p_4 tem o recurso r_3 e requer r_1 e r_4

Então o grafo de ocupação no instante t é o representado na Figura 16.

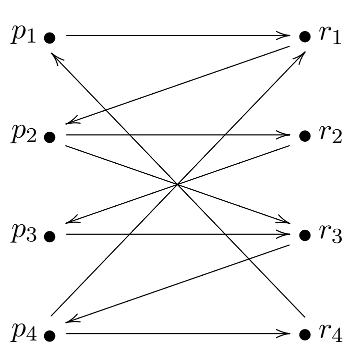
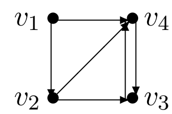


Figura 15: grafo do estado de ocupação dos recursos

Ocorre algum impasse? Por outras palavras, o grafo tem ciclos?

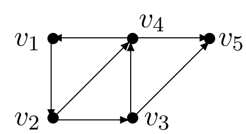
2.13 Exercícios.

1. Indique três caminhos elementares distintos de v_1 para v_3 no digrafo



   Qual a distância entre v_1 e v_3? Existe algum ciclo no grafo? O digrafo é transitivo?

2. Determine os graus fora e graus dentro dos vértices do grafo



   Indique todos os seus ciclos elementares. A partir dele obtenha um digrafo acíclico removendo um dos seus arcos. Faça uma listagem de todos os vértices que podem atingir todos os outros no digrafo dado.

3. Dado um digrafo simples $G = (V, A)$ em que condições é que a equação

$$d(v_1, v_2) + d(v_2, v_3) = d(v_1, v_3)$$

   é satisfeita por v_1, v_2, v_3 de V.

4. Para cada um dos digrafos dos exercícios 1 e 2, determine se são fortemente, fracamente ou unilateralmente conexos.

5. Mostre que um digrafo simples G é fortemente conexo se e só se existir um ciclo em G que inclui cada vértice pelo menos uma vez.

6. O diâmetro de um digrafo simples $G = (V, A)$ é dado por δ, onde $\delta = \max\limits_{u,v \in V} d(u, v)$. Determine o diâmetro do digrafo dos exercício 2.

7. Determine as componentes fortes do digrafo do exercício 2. Determine também as suas componentes unilaterais e fracas.

8. Mostre que todo o vértice e todo o arco de um grafo estão contidos em exactamente uma componente fraca.

9. Para cada um dos grafos dados, represente-o por um diagrama e diga se tem um ciclo de Euler, indicando-o no caso afirmativo.

   (a) $G = (V, E)$, onde $V = \{a, b, c, d, e, f, g\}$ e $E = \{\{a, a\}, \{a, b\}, \{b, c\}, \{b, g\}, \{c, g\}, \{g, f\}, \{f, d\}, \{d, e\}\}$

   (b) $G = (V, E)$, onde $V = \{v_1, v_2, v_3, v_4, v_5\}$ e $E = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_1, v_5\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_2, v_5\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_4, v_5\}\}$

   (c) $G = (V, E)$, onde $V = \{v_1, v_2, v_3, v_4, v_5\}$ e $E = \{\{v_1, v_3\}, \{v_1, v_4\}, \{v_3, v_4\}, \{v_2, v_4\}, \{v_2, v_5\}, \{v_4, v_5\}\}$

   (d) $G = (V, E)$, onde $V = \{a, b, c, d, e\}$ e $E = \{\{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, e\}, \{c, d\}, \{d, e\}\}$

3 Representação matricial de grafos

Seja $G = (V, E)$ um digrafo simples no qual $V = \{v_1, v_2, ..., v_n\}$ e os vértices se supõem ordenados de v_1 a v_n. A matriz A $n \times n$ de elementos a_{ij} dados por

$$a_{ij} = \begin{cases} 1 \text{ se } (v_i, v_j) \in E \\ 0 \text{ se } (v_i, v_j) \notin E \end{cases}$$

diz-se a *matriz das adjacências* do grafo G.

3.1 Observações.

1. A matriz de adjacências de $G = (V, E)$ é a matriz da relação E em V.

2. Recorde que toda a matriz cujos elementos são 0 e 1 ("falso"ou "verdadeiro") se diz uma *matriz booleana* ou *matriz bit*.

3. O número de elementos iguais a 1 na linha i da matriz de adjacências é igual ao grau fora de v_i e o número de elementos iguais a 1 na coluna j é igual ao grau dentro de v_j.

3.2 Exemplo. O grafo da Figura 16, onde os vértices se consideram ordenados por v_1, v_2, v_3, v_4, v_5, tem como matriz adjacente

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

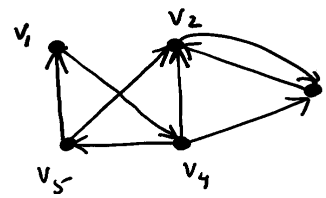


Figura 16: digrafo

Algumas propriedades de um grafo são imediatamente vistas através da sua matriz de adjacências. É o caso por exemplo da reflexividade e da simetria (Justifique).

Consideremos agora as potências da matriz de adjacências. Denotemos por $a_{ij}^{[2]}$ o elemento na posição ij da matriz A^2, sendo A a matriz de adjacências do exemplo anterior. Temos então

$$a_{ij}^{[2]} = \sum_{k=1}^{5} a_{ik}a_{kj}$$

Fazendo as contas, obtém-se

$$A^2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad \text{e} \quad A^3 = \begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 2 & 1 & 0 & 1 \end{bmatrix}$$

Consideremos a quarta linha de A. Os elementos não nulos são a_{42}, a_{43} e a_{45}, significando que (v_4, v_2), (v_4, v_3) e (v_4, v_5) são arestas do grafo. Ao multiplicar A por A, quando multiplicamos a quarta linha pela coluna j, temos a soma

$$a_{41}a_{1j} + a_{42}a_{2j} + a_{43}a_{3j} + a_{44}a_{4j} + a_{45}a_{5j}$$

onde cada uma das parcelas vai ser 1 ou 0. Por exemplo, seja $j = 2$; fica

$$[0\ 1\ 1\ 0\ 1][0\ 0\ 1\ \ 1\ 1]^t = 0 + 0 + 1 + 0 + 1\,.$$

O 1 na terceira parcela aparece porque temos

$$v_4 \longrightarrow v_3 \longrightarrow v_2$$

e o 1 da última parcela vem porque temos

$$v_4 \longrightarrow v_5 \longrightarrow v_2\,.$$

Cada 1 corresponde a um caminho de v_4 para v_2 de comprimento 2. Somando os dois 1's obtemos 2 que é o elemento $a_{42}^{[2]}$ e que é , portanto, o número de caminhos de comprimento 2 que temos de v_4 para v_2. De um modo geral, é válida a propriedade seguinte.

3.3 Teorema. *Seja A a matriz de adjacências de um digrafo G. O elemento da linha i e coluna j de A^n, $n \geq 0$, é igual ao número de caminhos de comprimento n do i-ésimo vértice para o j-ésimo vértice.*

Demonstração. Por indução sobre n. (Exercício)

Atendendo ao teorema anterior, se $G = (V, E)$ é um grafo e A é a matriz de adjacências, então, para um dado inteiro positivo r, a matriz

$$B_r = A^0 + A + A^2 + ... + A^r$$

permite determinar quantos caminhos de comprimento menor ou igual a r existem de um vértice v_i para um vértice v_j.

Recorde que num digrafo simples com n vértices o comprimento de um caminho ou ciclo elementar não excede n (Teorema 1 da Secção 2). Por outro lado, todo o caminho pode ser transformado num caminho elementar eliminando todos os ciclos do caminho (e, de forma análoga, todo o ciclo pode ser transformado num ciclo elementar). Assim, para determinar se existe algum caminho de v_i para v_j, precisamos apenas de averiguar se existem caminhos de comprimento menor ou igual a $n - 1$. Se $v_i = v_j$, existe sempre um caminho elementar de v_i para v_j, o caminho elementar $< v_i >$. Portanto, sendo G um grafo de n vértices, todos os caminhos elementares são contados pela matriz

$$B_n = A^0 + A + A^2 + ... + A^{n-1}\,.$$

Esta matriz permite portanto, dados dois vértices u e v, determinar se v é ou não atingível por u. (Justifique.)

A matriz de adjacências de um grafo não dirigido define-se de forma análoga. Ela é sempre uma matriz simétrica. (Porquê?)

Vamos agora definir outro tipo de matriz associada a um grafo.

Seja $G = (V, E)$ um digrafo simples tal que $|V| = n$ e os vértices de G, v_1, v_2, ..., v_n, se supõem ordenados por esta ordem. A matriz P $n \times n$ cujos elementos são dados por

$$p_{ij} = \begin{cases} 1, & \text{se existe um caminho de } v_i \text{ para } v_j \\ 0, & \text{se tal caminho não existe} \end{cases}$$

diz-se a *matriz dos caminhos* do grafo G.

A matriz dos caminhos pode ser calculada a partir da matriz $B_n = (b_{ij})$ (como definida atrás) pondo $p_{ij} = \text{sg} b_{ij}$, onde sg é a função sinal.

Se designarmos por $A^{(k)}$ a potência de ordem k de A relativamente ao produto booleano de matrizes, como já foi feito quando trabalhámos com matrizes de relações, temos que

$$P = A^{(0)} \vee A \vee A^{(2)} \vee A^{(3)} \vee ... \vee A^{(n-1)} = \bigvee_{k=0}^{n-1} A^{(k)}.$$

3.4 Exercícios.

1. Considere o grafo $G = (V, A)$, com $V = \{1, 2, 3, 4, 5\}$ e $A = \{a, b, c, d, e, f, g, h\}$, onde $a = \{1, 2\}, b = \{2, 3\}, c = \{3, 5\}, d = \{2, 5\}, e = \{2, 4\}, f = \{4, 5\}, g = \{1, 4\}, h = \{1, 5\}$. Determine:

   (a) A matriz de adjacências de G.

   (b) O grau de cada vértice.

   (c) A matriz dos caminhos de G.

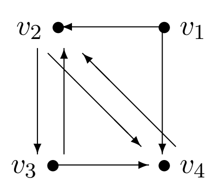
2. Um grafo G onde todos os vértices têm grau r designa-se por grafo *regular* de grau r.

   (a) Construa um grafo regular de grau 1 que não seja completo.

   (b) Construa um grafo regular de grau 2 que não seja completo.

   (c) Supondo que G é um grafo regular de grau r com n vértices, determine o número de arcos de G.

3. Determine a matriz de adjacências A do digrafo seguinte. Determine os caminhos de comprimento 1 e 2 de v_1 para v_4. Mostre que existe pelo menos um caminho simples de comprimento 4 de v_1 para v_4. Calcule A^2, A^3 e A^4 e comente os resultados anteriores, relacionando-os com as matrizes obtidas.



4. Mostre que a soma dos elementos da diagonal da segunda potência de uma matriz de adjacências de um grafo não dirigido G é o dobro do número de arcos de G.

5. Desenhe um grafo não dirigido cuja matriz de adjacências A verifique:

$$A^2 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 3 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix}.$$

   Em seguida, calcule A^3.

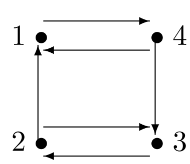
6. Mostre que toda a matriz booleana A verifica a igualdade

$$(I \vee A)^{(2)} = (I \vee A) \odot (I \vee A) = I \vee A \vee A^{(2)}$$

   onde I é a matriz identidade e $A^{(2)} = A \odot A$. Mostre também que, para todo o inteiro positivo r,

$$(I \vee A)^{(r)} = I \vee A \vee A^{(2)} \vee ... \vee A^{(r)}.$$

7. Relativamente ao grafo



   (a) Determine a matriz de adjacências A.

   (b) Obtenha a matriz de caminhos a partir de A.

8. Para um digrafo simples $G = (V, E)$, com $card(V) = n$, cuja matriz de adjacências é denotada por A, a sua *matriz de distâncias* é dada por

$$\begin{array}{ll} d_{ij} = \infty & \text{se } a_{ij}^{(}k) \notin A^{(k)},\ k = 0, 1, ..., n \\ d_{ii} = 0 & \text{para todo } i = 1, 2, ..., n \\ d_{ij} = k & \text{onde } k \text{ é o menor inteiro para o qual } a_{ij}^{(k)} \neq 0 \end{array}$$

   Determine a matriz de distâncias do digrafo do exercício 3. O que significa $d_{ij} = 1$?

9. Mostre que um digrafo G é fortemente conexo se todas as entradas da matriz das distâncias são diferentes de ∞. Como se pode obter a matriz dos caminhos a partir da matriz das distâncias? Como se modificam as entradas da diagonal?

4 Árvores

Existem duas grandes classes de árvores: *árvores livres* e *árvores com raiz.* Uma árvore com raiz é um caso especial de grafo dirigido. As árvores binárias (com raiz) foram já estudadas.

Uma árvore livre, ou apenas *árvore* é um grafo não dirigido simples, conexo e acíclico. Uma árvore tem de ter pelo menos um vértice (visto ser um grafo conexo). Na Figura 17 estão representadas algumas árvores.

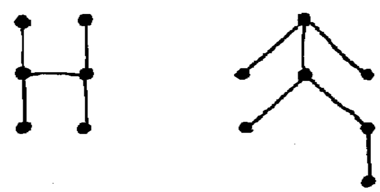


Figura 17: árvores

4.1 Teorema. *Uma árvore com n vértices tem $n-1$ arestas.*

Demonstração. Por indução sobre n. Para $n = 1$, é claro que a árvore tem 0 arestas.

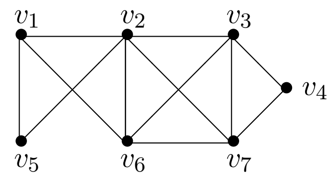
Suponhamos a propriedade válida para n e provemos que se verifica para $n+1$. Numa árvore de $n+1$ vértices consideremos um caminho acíclico $< v_1, v_2, ..., v_m >$ com os vértices todos diferentes e tal que não existe nenhum caminho do grafo que contenha este estritamente. Então os vértices v_1 e v_m têm ambos grau igual a um. (Porquê?) Tiremos do grafo o vértice v_1 e a aresta incidente em v_1. Obtemos assim um grafo de n vértices que, por hipótese indutiva, tem $n-1$ arestas. Consequentemente, o grafo inicial que se obtém deste juntando-lhe v_1 e a aresta que lhe era incidente, tem n arestas.

Uma árvore *abrangente* de um grafo não dirigido conexo $G = (V, A)$ é uma árvore livre cujo conjunto de vértices é V e que é um subgrafo de G.

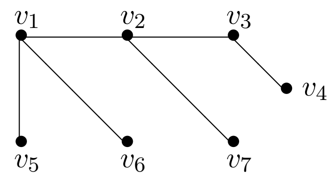
Técnicas para gerar uma árvore abrangente de um dado grafo:

1. Tirar arestas que pertencem a ciclos, uma a uma até o grafo não ter ciclos simples.

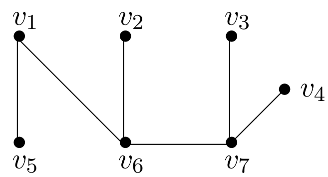
   Exemplo: Uma árvore abrangente para o grafo

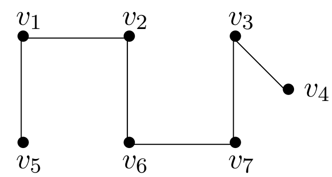


é a seguinte:



Outras árvores abrangentes geradas pelo mesmo grafo:





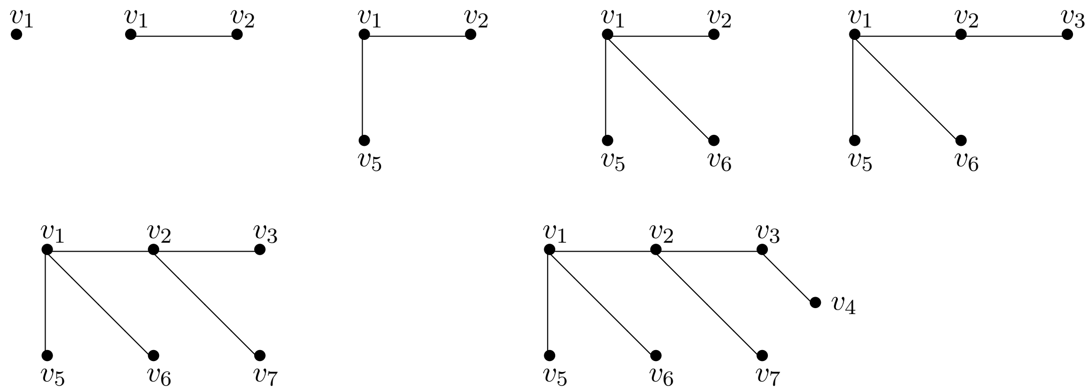
2. Escolher uma sequência de $n-1$ arestas, uma a uma, de tal modo que em cada passo o subgrafo obtido é acíclico (supondo que o grafo tem n vértices).

   Exemplo: Consideremos o grafo do exemplo anterior. Vamos primeiro escrever uma *lista de adjacências*, i.e., uma lista que para cada vértice indica os vértices que lhe estão ligados por meio de uma aresta:

$$\begin{aligned}
v_1 &: v_2,\ v_5,\ v_6\\
v_2 &: v_1,\ v_3,\ v_5,\ v_6,\ v_7\\
v_3 &: v_2,\ v_4,\ v_6,\ v_7\\
v_4 &: v_3,\ v_7\\
v_5 &: v_1,\ v_2\\
v_6 &: v_1,\ v_2,\ v_3,\ v_7\\
v_7 &: v_2,\ v_3,\ v_4,\ v_6
\end{aligned}$$

Para gerar uma árvore abrangente, comecemos pelo vértice v_1. Os vértices aos quais v_1 se liga são v_2, v_5, v_6. Temos então as arestas $\{v_1, v_2\}$, $\{v_1, v_5\}$ e $\{v_1, v_6\}$. Várias escolhas poderíamos fazer agora: podíamos partir de v_2, v_5 ou v_6. Escolhemos a ordem dos índices das letras que designam os vértices. Portanto, escolhemos v_2 e, das arestas ligadas a v_2, escolhemos $\{v_2, v_3\}$ e $\{v_2, v_7\}$, pois com todas as outras obteríamos ciclos. Passamos a v_3 e seleccionamos apenas $\{v_3, v_4\}$, pois todas as outras escolhas formariam ciclos. Neste momento, temos já uma árvore abrangente do grafo.

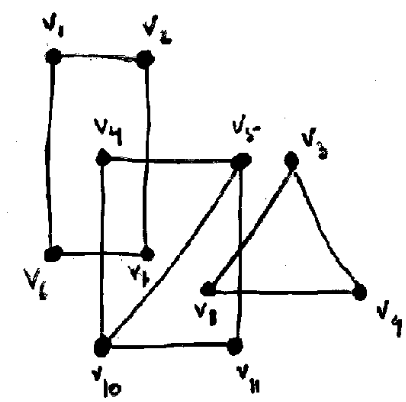
A seguir é dado um esquema dos passos seguidos:



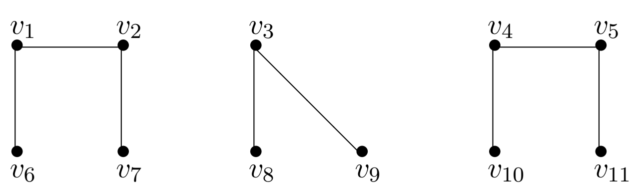
Uma *floresta* é um grafo $G = (V, E)$ tal que $V = \bigcup_{i \in I} V_i$, sendo os V_i's disjuntos dois a dois, $A = \bigcup_{i \in I} A_i$ sendo os A_i's disjuntos dois a dois, e, para cada $i \in I$, $G_i = (V_i, A_i)$ é uma árvore.

Dado um grafo não conexo, em vez de gerarmos uma árvore abrangente para esse grafo, geramos uma floresta. Assim, uma *floresta abrangente* de um grafo não dirigido é a floresta obtida substituindo cada uma das componentes conexas por uma árvore abrangente dessa componente.

4.2 Exemplo. Dado o grafo



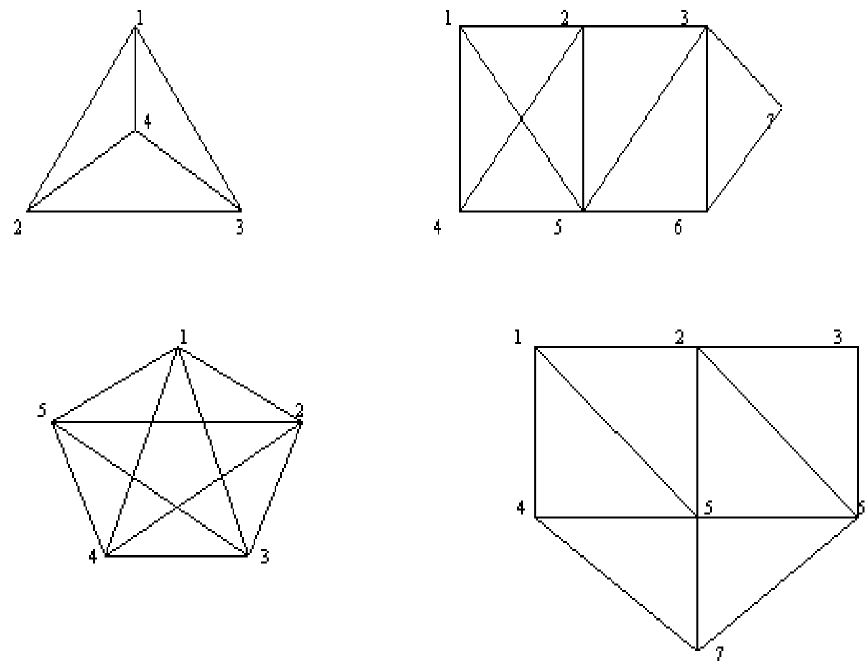
uma sua floresta abrangente é



4.3 Exercícios.

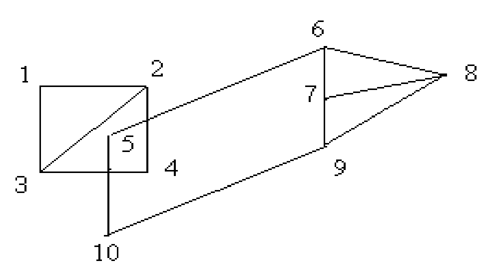
1. Determine todas as árvores livres distintas com dois, três e quatro vértices.

2. Determine uma árvore abrangente para cada um dos grafos seguintes, removendo sucessivamente arestas de ciclos simples.



3. O mesmo que no exercício anterior por um processo diferente, nomeadamente, escolhendo uma sequência com um número conveniente de arestas, onde as arestas são tomadas uma a uma, de tal modo que o subgrafo que se obtém em cada passo é acíclico. Desenhe uma sequência de grafos que ilustre o procedimento seguido.

4. Determine uma floresta abrangente para o grafo.



5 Grafos com pesos

Um *grafo com pesos* é um grafo que tem um peso, i.e., um número, associado a cada aresta. A Figura 18 representa um grafo com pesos. O peso da aresta $\{a, b\}$ é $p(\{a, b\}) = 2$, o

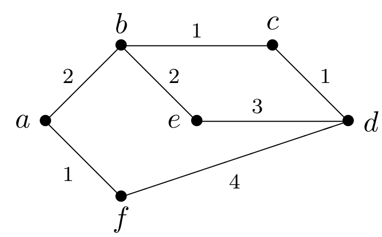


Figura 18: grafo com pesos

peso da aresta $\{b, c\}$ é $p(\{b, c\}) = 1$, etc.

Num grafo com pesos, dado um caminho

$$C = \{\{v_0, v_1\}, \{v_1, v_2\}, ..., \{v_{k-1}, v_k\}\}$$

de v_0 para v_k, o *comprimento do caminho*, também chamado *peso do caminho*, é a soma dos pesos das arestas que o constituem. Assim o comprimento de C é

$$p(C) = p(\{v_0, v_1\}) + p(\{v_1, v_2\}) + ... + p(\{v_{k-1}, v_k\}) .$$

Neste contexto, um *caminho mais curto* de v_0 para v_k é um caminho de peso mínimo; a *distância de* v_0 *a* v_k é o peso dum caminho mais curto. Por exemplo, no grafo da Figura 18 o caminho mais curto de c para e é $< c, b, e >$ e o seu peso é 1+2=3; portanto, a distância de c a e é 3.

5.1 Algoritmo de Dijkstra para determinar um caminho mais curto entre dois vértices de um grafo com pesos.

Consideremos ainda o grafo da Figura 19. É claro que é fácil determinar a distância entre a e d. Uma observação atenta do grafo leva à conclusão de que um caminho mais curto é $< a, b, c, d >$ e que a distância é igual a 4. Mas em problemas da vida real podemos ter grafos com pesos com um número muito grande de vértices e arestas, o que dificulta a determinação das distâncias. Existem vários algoritmos para o cálculo da distância entre dois vértices, vamos aqui debruçar-nos sobre um deles, o algoritmo de Dijkstra.

Antes de descrever o algoritmo, vamos ilustrá-lo com o cálculo da distância de a a d no grafo da Figura 19. Simultâneamente pode ir verificando na Tabela 19 o método que vamos seguindo.

Vamos proceder do seguinte modo: Partimos de a e vamos juntando passo a passo outros vértices a a, e arestas, até chegar a d. Em cada passo, temos um certo sugrafo do grafo dado, constituído por esses vértices e arestas. Tal subgrafo é construído de forma que ele nos dá um caminho mais curto (no grafo inicial) de a a cada um dos vértices do subgrafo. Vamos utilizar uma função L tal que:

inicialmente $L(a) = 0$ e $L(x) = \infty$ para todos os $x \neq a$;
a seguir, para cada vértice seleccionado y, temos

$$L(x) := \min\{L(x),\, L(y) + p(y,x)\}$$

onde

$$p(y,x) = p(\{y,x\}).$$

Após o passo em que juntamos o vértice d, obtemos $L(d)$ que nos dá a distância de a a d.

Partimos então de

$$a$$

Um caminho a começar em a tem de passar por b e f visto estes serem os vértices adjacentes a a. Agora

$$L(b) = L(a) + p(a,b) = 2 \text{ e } L(f) = L(a) + p(a,f) = 1$$

Como

$$1 < 2$$

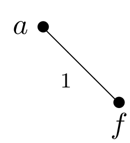
escolhemos

$$f$$

e a aresta

$$\{a,f\}.$$

O sugrafo obtido é



Um caminho que contenha esta como primeira aresta e continue a juntar arestas distintas passa a seguir por d. Temos que, indo de a a d deste modo, o comprimento do caminho percorrido é

$$L(d) = L(f) + p(f,d) = 1 + 4 = 5$$

Mas, dentro dos vértices x ainda não seleccionados, o valor mínimo de $L(x)$ ´´e atingido por

$$L(b) = 2$$

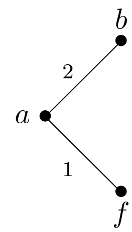
Então retomamos o caminho que passa por b, e que tinhamos abandonado temporariamente. Ou seja, é então agora altura de seleccionar o vértice

$$b$$

e a aresta

$$\{a, b\}$$

Obtemos então o subgrafo



Continuando, os vértices que ainda não foram seleccionados e são adjacentes a b são c e e. E temos

$$L(c) = L(b) + p(b, c) = 2 + 1 = 3 \ \text{ e } \ L(e) = L(b) + p(b, e) = 2 + 2 = 4$$

Como

$$3 < 4,\ 5$$

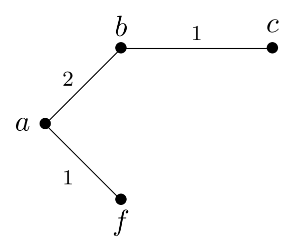
seleccionamos o vértice

$$c$$

e a aresta

$$\{b, c\}$$

O subgrafo resultante é:



Neste momento, de entre os vértices ainda não seleccionados, o único adjacente a c é o vértice d, e tem-se

$$L(d) := \min\{L(d), L(c) + p(c, d)\} = 4$$

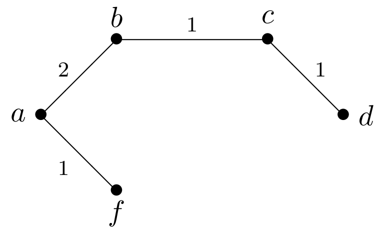
Como

$$4 \leq 4, 5$$

podemos seleccionar

$$d \ \text{ e } \ \{c, d\}$$

(também se podia seleccionar e e $\{b, e\}$, visto que $L(e) = L(b) + p(b, e)$ também é igual a 4.) Obtemos o subgrafo



Este sugrafo (que é uma árvore), dá-nos, para cada um dos seus vértices x, um caminho mais curto de a para x no grafo inicial. Em particular,

$$< a, b, c, d > \text{ é um caminho mais curto de } a \text{ para } d \text{ e } d(a, b) = 4.$$

O procedimento acabado de seguir para encontrar a distância de a a d chama-se algoritmo de Djkstra. Ilustramos os passos acabados de descrever na tabela seguinte, onde, em cada passo, S designa o conjunto dos vértices do subgrafo obtido, e R designa o conjunto das arestas desse subgrafo. Em cada linha vamos adicionando elementos a S e R.

S	R	$L(x), x \notin S$
		$L(a) := 0$, $L(x) := \infty$, $x \neq a$
a		$L(b) := 2$, $L(f) = 1$, $L(x) := \infty, x \neq b, f$
f	$\{a, f\}$	$L(d) := L(f) + p(f, d) = 5$,
b	$\{a, b\}$	$L(c) := L(b) + p(b, c) = 3$, $L(e) := L(b) + p(b, e) = 4$
c	$\{b, c\}$	$L(d) := \min\{L(d),\, L(c) + p(c, d)\} = 4$
d	$\{c, d\}$	$L(d) = d(a, d) = 4$

Figura 19: Tabela 1

No que se segue, dados quaisquer dois vértices de um grafo com pesos, usamos a expressão $p(u, v)$ com o seguinte significado:

$$p(u, v) = \begin{cases} \text{peso da aresta } \{u, v\}, & \text{se ela pertence ao grafo} \\ \infty, & \text{se } \{u, v\} \text{ não pertence ao grafo} \end{cases}$$

Descreve-se a seguir o algoritmo de Dijkstra, acabado de exemplificar, para determinar a distância e um caminho mais curto entre os vértices a e z de um grafo com pesos:

1. $L(a) := 0$

2. $L(x) := \infty$, $x \neq a$
3. $S := \emptyset$

$3'$. $R := \emptyset$

4. Se $z \in S$, vai-se para 9.; se $z \notin S$, continua-se em 5.
5. Escolhe-se um vértice v tal que $L(v) = \min_{x \notin S} L(x)$
6. $S := S \cup \{v\}$

$6'$. $R := R \cup \{$última aresta usada para a realização do peso mínimo $p\{u, v\}\}$

7. $L(x) := \min\{L(x), L(v) + p(v, x)\}$ para todo o vértice x
8. Vai para 4.
9. $L(z) =$ distância de a a z

Note que (S,R) é uma árvore com pesos que dá um caminho mais curto de a para cada um dos vértices da árvore.

A seguir vamos demonstrar que o algoritmo de Dijkstra calcula a distância de a a z. Mais do que isso, em cada passo 4 do algoritmo de Dijkstra, $L(v)$ é o comprimento de um caminho mais curto de a a v.

5.2 Teorema. *O algoritmo de Dijkstra determina o comprimento de um caminho mais curto entre dois vértices de um grafo com pesos.*

Demonstração. Sejam a e z dois vértices de um grafo com pesos. Vamos provar por indução sobre i que $P(i)$:=(na i-ésima vez que chegamos ao passo 4 do algoritmo de Dijkstra, $L(v)$ é o comprimento de um caminho mais curto de a a v).

Base indutiva: Na primeira vez que se chega ao passo 4, escolhe-se a e $L(a) = 0$. Logo $L(a)$ é igual ao comprimento dum caminho mais curto de a a a.

Hipótese indutiva: A propriedade $P(k)$ verifica-se para todo o $k < i$.

Passo indutivo: Suponhamos que estamos no passo 4 pela k-ésima vez e escolhemos $v \notin S$ tal que o valor de $L(v)$ é mínimo.

No que se segue quando nos referirmos a $L(v)$ estamos a considerar o valor de $L(v)$ na k-ésima vez que passamos no passo 4. Primeiro mostramos que, se existir um caminho de a para um vértice w cujo comprimento é menor do que o valor de $L(v)$, então $w \in S$ (i.e., w foi seleccionado na i-ésima vez que passamos no passo 4, para algum $i < k$). Seja P um caminho de a para w de comprimento menor do que $L(v)$. Suponhamos, por contradição, que $w \notin S$. Seja x o vértice mais próximo de a em P que não pertence a S, e seja u o predecessor de x em P. Então $u \in S$, pelo que u foi escolhido no passo 4 durante uma iteração anterior. Mas por hipótese indutiva $L(u)$ é o comprimento dum caminho mais curto de a para u. Temos então que

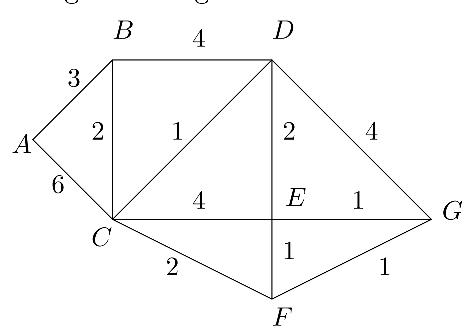
$$L(x) \leq L(u) + p(u,x) \leq \text{comprimento de } P < L(v)\,.$$

Mas esta desigualdade mostra que, ao chegar pela k-ésima vez ao passo 4, v não é o vértice fora de S com valor mínimo para $L(v)$ ($L(x)$ é menor). Esta contradição mostra que w tem de pertencer a S.

Em particular, acabámos de mostrar que se existisse um caminho de a para v de comprimento menor do que $L(v)$, v teria sido já seleccionado no passo 4 (antes da k-ésima passagem) e incluído em S. Consequentemente, todo o caminho de a para v tem comprimento maior ou igual a $L(v)$. Por construção, existe um caminho de a para v de comprimento $L(v)$, logo este é um caminho mais curto de a para v. Fica assim completa a prova.

Se além da distância, pretendemos a árvore correspondente a um caminho mais curto de a para z, podemos juntar ao algoritmo a construção dessa árvore T, onde os vértices de T são os elementos de S e as arestas são aquelas cujo peso entra no cálculo do mínimo referido no passo 4. No exemplo a seguir introduzem-se os passos $3'$ e $5'$ onde se constrói o conjunto R constituído pelas arestas de T:

5.3 Exemplo. Uso do algoritmo de Dijkstra para encontrar a distância e um caminho óptimo entre os vértices A e G do grafo da figura



(Vão tomar-se os vértices por ordem alfabética; assim, quando L(v) toma o valor mínimo para mais do que um vértice, escolhe-se o que fica em primeiro lugar no alfabeto.)

A descrição da aplicação do algoritmo a seguir apresentada é disposta num quadro no final (ver Figura 5.3).

1. $L(A) := 0$

2. $L(X) := \infty$, $X \neq A$

3. $S := \emptyset$

$3'$. $R := \emptyset$

4. $L(A) = \min_{X \in S} L(X)$

5. $S := S \cup \{A\} = \{A\}$

5′. $R := R \cup \emptyset = \emptyset$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(A) + p(A, X)\}$; logo $L(B) = \min\{\infty, 3\} = 3$, $L(C) = \min\{\infty, 6\} = 6$, $L(X) = \infty$ para $X \neq A, B, C$

4. $L(B) = \min_{X \in S} L(X) = 3$

5. $S := S \cup \{B\} = \{A, B\}$

5′. $R := R \cup \{\{A, B\}\} = \{\{A, B\}\}$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(B) + p(B, X)\}$; logo $L(C) = \min\{6, 3 + 2\} = 5$, $L(D) = \min\{\infty, 3 + 4\} = 7$, $L(X) = \infty$ para $X \neq A, B, C, D$

4. $L(C) = \min_{X \in S} L(X) = L(B) + p(B, C) = 5$

5. $S := S \cup \{C\} = \{A, B, C\}$

5′. $R := R \cup \{\{B, C\}\} = \{\{A, B\}, \{B, C\}\}$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(C) + p(C, X)\}$; logo $L(D) = \min\{7, 5 + 1\} = L(C) + p(C, D) = 6$, $L(E) = \min\{\infty, 5 + 4\} = 9$, $L(F) = \min\{\infty, 5 + 2\} = 7$, $L(G) = \infty$

4. $L(D) = \min_{X \in S} L(X) = L(C) + p(C, D) = 6$

5. $S := S \cup \{D\} = \{A, B, C, D\}$

5′. $R := R \cup \{\{C, D\}\} = \{\{A, B\}, \{B, C\}, \{C, D\}\}$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(D) + p(D, X)\}$; logo $L(G) = \min\{\infty, 10\} = 10$, $L(E) = \min\{9, 6 + 2\} = 8$ e $L(F) = 7 = L(C) + p(C, F)$

4. $L(F) = \min_{X \in S} L(X) = L(C) + p(C, F) = 7$

5. $S := S \cup \{F\} = \{A, B, C, D, F\}$

5′. $R := R \cup \{\{C, F\}\} = \{\{A, B\}, \{B, C\}, \{C, D\}, \{C, F\}\}$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(F) + p(F, X)\}$; logo $L(G) := \min\{10, 7 + 1\} = 8$ e $L(E) := \min\{8, 7 + 1\} = 8 = L(D) + p(D, E)$

4. $L(E) = \min_{X \notin S} L(X) = 8 = L(D) + p(D, E)$

5. $S := S \cup \{E\} = \{A, B, C, D, E, F\}$

5′. $R := R \cup \{\{D, F\}\} = \{\{A, B\}, \{B, C\}, \{C, D\}, \{C, F\}, \{D, E\}\}$

6. $G \notin S$

7. $L(X) := \min\{L(X), L(E) + p(E, X)\}$; logo $L(G) = \min\{8, 8 + 1\} = 8 = L(F) + p(F, G)$

4. $L(G) = \min_{X \notin S} L(X) = L(F) + p(F, G) = 8$

5. $S := S \cup \{G\} = \{A, B, C, D, E, F, G\}$

5′. $R := R \cup \{\{F, G\}\} = \{\{A, B\}, \{B, C\}, \{C, D\}, \{C, F\}, \{F, E\}, \{F, G\}\}$

6. $G \in S$

9. $L(G)$=distância de A a G.

A árvore $T = (S, R) = (\{A, B, C, D, E, F, G\}, \{\{A, B\}, \{B, C\}, \{C, D\}, \{C, F\}, \{D, E\}, \{F, G\}\})$ dá um caminho mais curto no grafo dado de A para cada um dos vértices pertencentes à árvore. Assim um caminho mais curto de A a G é $< A, B, C, F, G >$.

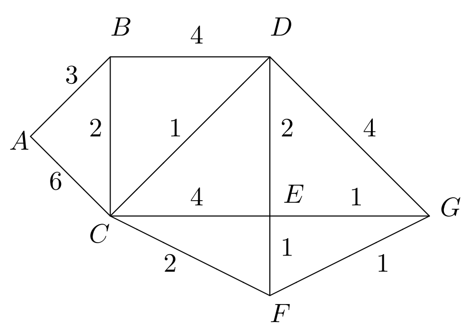
O desenvolvimento do algoritmo feito para este exemplo pode ser exposto num quadro como ilustrado a seguir:

S	R	$L(X), X \notin S$
		$L(A) = 0,\ L(X) = \infty,\ X \neq A$
A		$L(B) = p(A,B) = 3,\ L(C) = p(A,C) = 6,$ $L(X) = \infty, X \neq B, C$
B	$\{A,B\}$	$L(C) = \min\{6, L(B) + p(B,C)\} = 5,$ $L(D) = L(B) + p(B,D) = 7,$ $L(X) = \infty, X \neq C, D$
C	$\{B,C\}$	$L(D) = \min\{7, L(C) + p(C,D)\} = 6,$ $L(E) = L(C) + p(C,E) = 9,$ $L(F) = L(C) + p(C,F) = 7,$ $L(G) = \infty$
D	$\{C,D\}$	$L(E) = \min\{9, L(D) + p(D,E)\} = 8,$ $L(G) = L(D) + p(D,G) = 10$
F	$\{C,F\}$	$L(E) = \min\{8, L(F) + p(F,E)\} = 8 = L(D) + p(D,E)$ $L(G) = \min\{10, L(F) + p(F,G)\} = 8$
E	$\{D,E\}$	$L(G) = \min\{8, L(E) + p(E,G)\} = 8 = L(F) + p(F,G)$
G	$\{F,G\}$	$L(G) = 8 = d(A,G)$

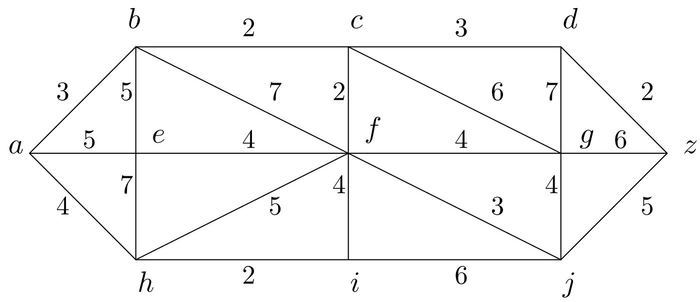
5.4 Exercícios.

1. Use o algoritmo de Dijkstra para encontrar a distância entre os vértices A e H do grafo com pesos $\mathcal{G} = (\mathcal{V}, \mathcal{A}, p)$ onde $\mathcal{V} = \{A,B,C,D,E,F,G,H\}$, $\mathcal{A} = \{\{A,B\},\{A,F\},\{B,C\},$ $\{B,E\},\ \{B,D\},\{C,E\},\{C,H\},\{D,E\},\{D,F\},\{E,G\},\{F,G\},\{G,H\}\}$ e os pesos das arestas são $p(\{A,B\}) = 2$, $p(\{A,F\} = 1$, $p(\{B,C\}) = 2$, $p(\{B,E\} = 4$, $p(\{B,D\}) = 4$, $p(\{C,E\}) = 3$, $p(\{C,H\}) = 1$, $p(\{D,E\}) = 4$, $p(\{D,F\}) = 3$, $p(\{E,G\}) = 7$, $p(\{F,G\}) = 5$, $p(\{G,H\}) = 6$.

2. Use o algoritmo de Dijkstra para encontrar um caminho óptimo entre os vértices A e G do grafo da figura



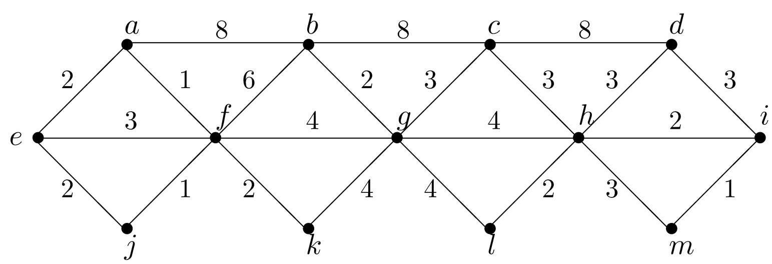
3. Determine o comprimento de um caminho mais curto e esse caminho mais curto entre os dois vértices dados no grafo com pesos da figura.



(a) a, f (b) a, g (c) a, z (d) b, j (e) h, d

4. Escreva um algoritmo que determine a distância entre dois vértices de um grafo com pesos conexo e que determine também um caminho mais curto.

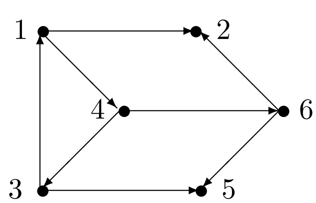
5. Relativamente ao grafo com pesos da figura, use o algoritmo de Dijkstra para determinar a distância e um caminho mais curto de b para h.



6 Exercícios

1. Averigue se o grafo $(\{1, 2, 3, 4, 5\}, \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\})$ tem algum ciclo de Euler. Em caso negativo, justifique; em caso afirmativo, indique um ciclo de Euler do grafo.

2. Considere o grafo seguinte



   (a) Seja A a matriz de adjacências de G. Escreva A, considerando os vértices ordenados pela ordem habitual.

   (b) Diga, justificando e sem calcular as matrizes:

   i) qual o elemento na posição 4,5 de A^2;

   ii) qual o elemento na posição 1,2 de $A + A^2 + A^3$;

(c) Determine as componentes fracas, as componentes unilaterais e as componentes fortes do grafo.

3. (a) Defina caminho e ciclo entre dois vértices dum digrafo. Quando se diz que um ciclo é elementar?

   (b) O digrafo da questão anterior tem ciclos? Se sim indique um ciclo elementar do digrafo.

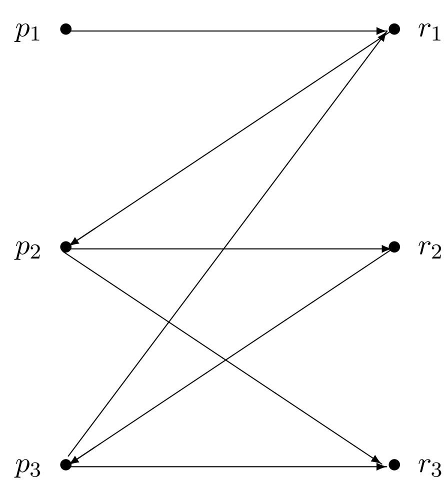
   (c) Prove que num digrafo simples com n vértices o comprimento de um caminho elementar é menor ou igual do que $n-1$.

4. Complete a demonstração seguinte de que as componentes fortes de um digrafo determinam uma partição dos seus vértices (Note que essa demonstração tem de ser completada em duas partes do texto assinaladas por "...(1)..."e "...(2)...". Na sua folha de respostas só deve ser escrito o que falta em (1) e (2) para que a demonstração fique completa.):

   Demonstração. Seja $G = (V, E)$ um digrafo, seja $v \in V$ e seja S o conjunto de todos os vértices u de G tais que existe um caminho de v para u e existe um caminho de u para v. É claro que o subgrafo de G induzido por S é fortemente conexo. Além disso, não existe nenhum subgrafo de G que o contenha propriamente e também seja fortemente conexo. Com efeito, se $S \subseteq H$ e o subgrafo induzido por H também é fortemente conexo, então, dado $w \in H$, ... (1) ..., pelo que $w \in S$ e, portanto, $S = H$.

   Resta mostrar que v não pode pertencer a outra componente forte diferente de S. ... (2) ...

5. Considere o grafo seguinte



(a) Determine a sua matriz de adjacências considerando os vértices ordenados por p_1, p_2, p_3, r_1, r_2, r_3.

(b) Diga, justificando, se o grafo é bipartido.

(c) O grafo tem ciclos? Se sim, indique um deles.

(d) Suponha que o grafo representa o estado de utilização de recursos de um sistema operativo no instante t, sendo p_1, p_2 e p_3 programas e r_1, r_2 e r_3 recursos. Diga, justificando, se se verifica algum impasse.

(e) Determine as componentes fracas, as componentes unilaterais e as componentes fortes do grafo.

6. Seja G o grafo com pesos que tem $\{a, b, c, d\}$ por conjunto de vértices, $\{\{a, b\}, \{a, c\}, \{b, d\}, \{c, d\}\}$ por conjunto de arestas, e o peso das arestas é dado por $p(\{a, b\}) = 2$, $p(\{b, d\}) = 2$, $p(\{a, c\}) = 2$, $p(\{c, d\}) = 1$.

   (a) Represente o grafo.

   (b) Indique um caminho mais curto entre a e d.

   (c) Descreva o algoritmo de Dijkstra para determinar a distância de a a d. (Considere que os vértices estão ordenados por ordem alfabética.)

7. Considere a seguinte matriz de adjacências de um digrafo de vértices 1, 2, 3, 4, 5, considerando os vértices ordenados pela ordem natural:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

   (a) Desenhe o digrafo colocando os vértices 1, 2 e 3 numa linha horizontal e os vértices 4 e 5 noutra linha horizontal por baixo da anterior.

   (b) Diga, justificando, qual a distância entre o vértice 1 e 4.

   (c) Sem calcular as matrizes diga, justificando, qual a entrada na posição 1,4 nas matrizes A^3 e A^4.

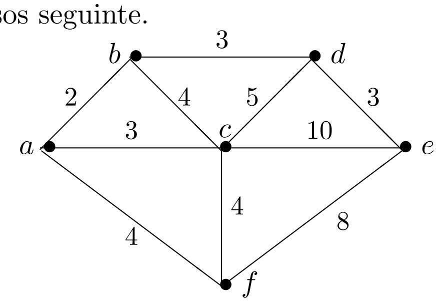
   (d) Diga, justificando, se o grafo é fortemente conexo, unilateralmente conexo ou fracamente conexo.

   (e) Determine as componentes fracas, unilaterais e fortes do grafo.

   (f) Sem calcular a matriz, diga justificando quantos zeros tem a matriz dos caminhos do grafo.

(g) Defina ciclo de Euler. Em seguida diga, justificando, se o multigrafo não dirigido obtido do digrafo dado considerando cada aresta como uma aresta não dirigida tem ou não algum ciclo de Euler.

8. Considere o grafo com pesos seguinte.



(a) Aplique-lhe o algoritmo de Dijkstra considerando no início $L(a) = 0$ e $L(x) = \infty$ para $x \neq a$ e acabando apenas quando S contiver todos os vértices do grafo. Indique também em cada passo as arestas envolvidas. Pode apresentar os vários passos num quadro com três colunas, uma para S, outra para R (arestas) e outra para os valores de $L(x)$.

(b) Usando o feito na alínea anterior,

(i) desenhe a árvore com pesos obtida com o algoritmo,

(ii) indique a distância de a a e,

(iii) indique um caminho mais curto de a para e e outro de a para f.

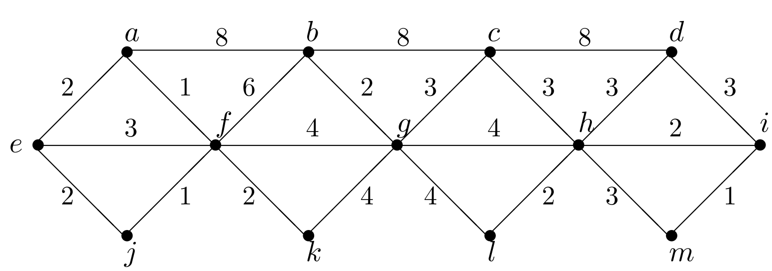
9. Seja G um grafo e A a sua matriz de adjacências.

(a) Dado $k \in \mathbb{N}$, que informação dá a potência booleana $A^{(k)}$?

(b) Qual o comprimento máximo de um caminho elementar entre dois vértices diferentes de um grafo de n vértices?

(c) Suponha que o conjunto de vértices de G é $\{v_i : 1 \leq i \leq 20, i \in \mathbb{N}\}$. Justifique a afirmação seguinte num texto de entre 5 a 10 linhas: "A matriz dos caminhos de G é dada por $\bigvee_{i=0}^{19} A^{(k)}$."

10. Relativamente ao grafo com pesos da figura, use o algoritmo de Dijkstra para determinar a distância e um caminho mais curto de b para h.



11. A matriz dos caminhos de um digrafo G de vértices v_1, v_2, v_3 e v_4 (considerados por esta ordem) é $P = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$.

    (a) Defina matriz de caminhos de um grafo.

    (b) Diga, justificando, se o grafo G (cuja matriz dos caminhos é P) é fortemente conexo, unilateralmente conexo ou conexo.

    (c) Indique os vértices de cada uma das componentes fortemente conexas.

12. Uma rede rodoviária entre seis povoações, A, B, C, D, E e F, é constituída por oito estradas como descrito a seguir:

    entre A e B com 30Km; entre A e C com 22Km; entre A e D com 30Km;

    entre B e E com 20Km; entre C e E com 12Km; entre C e D com 36Km;

    entre E e F com 40Km; entre D e F com 18Km.

    Represente esta rede rodoviária por um grafo com pesos. Em seguida aplique o algoritmo de Dijkstra ao grafo para determinar o percurso mais curto da povoação D para a povoação B, bem como a respectiva distância.

13. (a) Desenhe um digrafo de vértices 1, 2 e 3 cuja matriz de adjacências A satisfaz a igualdade $A^3 = I$.

    (b) Indique o conjunto de arestas de um digrafo de vértices 1, 2, ..., n cuja matriz de adjacências A satisfaz a igualdade $A^n = I$.

14. Considere o digrafo $G = (V, E)$ onde $V = \{a, b, c, d, e\}$ e $E = \{(a, b), (a, d), (b, c), (b, e), (c, e), (d, b), (e, d)\}$.

    (a) Desenhe o grafo G, colocando os vértices a, b e c numa mesma linha horizontal em cima e d e e numa mesma linha horizontal em baixo.

    (b) Indique a matriz de adjacências de G, considerando os vértices ordenados pela sua ordem alfabética, e denotando-a por A.

    (c) Sem calcular as matrizes diga, justificando, qual a entrada na posição 2,4 nas matrizes A^3 e A^4.

    (d) Determine as componentes fortes do grafo G.

    (e) Desenhe o grafo não dirigido com pesos que resulta de tirar as setas às aresta do grafo G e atribuir-lhe os seguintes pesos:

o peso de $\{a, b\}$ é 1; o peso de $\{a, d\}$ é 3; o peso de $\{b, c\}$ é 2; o peso de $\{b, d\}$ é 1;

o peso de $\{b, e\}$ é 7; o peso de $\{c, e\}$ é 3; o peso de $\{d, e\}$ é 5.

Use o algoritmo de Dijkstra para determinar a distância e um caminho mais curto de a a e. (Considere que os vértices estão ordenados por ordem alfabética.)

15. Seja $G = (V, A)$ um grafo não dirigido simples (sem pesos)

    (a) Diga quando se diz que um caminho de G é elementar.

    (b) Sabendo que G tem n vértices, mostre que um caminho elementar de G entre dois vértices diferentes tem comprimento menor ou igual a $n - 1$.

    (c) Mostre que a relação P definida por xPy := *existe um caminho de* x *para* y, definida no conjunto V dos vértices de G, é uma relação de equivalência.

Bibliografia

M. O. Albertson e J. P. Hutchinson, *Discrete Mathematics with Algorithms*, John Wiley Sons, 1988.

R. E. Davis Truth, *Deduction and Computation*, Computer Science Press, 1989.

W. K. Grassmann e J.-P. Tremblay, *Logic and Discrete Mathematics - A Computer Science Perspective*, Prentice Hall, 1996.

Halmos, Paul Richard, *Teoria Ingénua dos Conjuntos*, Editora da Univ. S. Paulo e Editora Polígono, 1970.

J. Hein, *Discrete Structures*, Logic and Computability, Jones and Bartlett, 1995.

R. Johnsonbaugh, *Discrete Mathematics*, Prentice Hall, 1993.

H. F. Mattson, Jr., *Discrete Mathematics*, John Wiley Sons, 1993.

Elliot Mendelson, *Introduction to Mathematical Logic*, Chapman & Halll/CRC, Fourth Edition, 1997.

K. Rosen, *Discrete Mathematics and its Applications*, MacGraw-Hill, 1999.